

EXHIBIT 5

The Right To Be Forgotten

Criminal Law & Procedure Practice Group Teleforum



Oct
5
2018
Friday
12:30 p.m.
EDT

Topics:

Civil Rights • Corporations, Securities & Antitrust • Criminal Law & Procedure • International Law & Trade • Litigation

Sponsors:

Criminal Law & Procedure Practice Group

 In-Person Event

Teleforum

LISTEN & DOWNLOAD

Download

The “right to be forgotten” refers to the right of individuals to have a company remove or delete their personal data when the company has no apparent justification for continuing to keep it. The “right to be forgotten” was established by the European Court of Justice in 2014, when it ruled that individuals had the right to request the removal of links to either irrelevant or outdated materials. Over half a million requests for link removals have occurred since the ruling, of which Google acquiesced to nearly half.

Earlier this year, the High Court of Great Britain ruled against Google in a landmark court case, and sided in favor of advocates for the right to be forgotten, ruling that Google had to comply with a businessman who requested his previous criminal record of a sentence served over a decade previously be removed from the search engine.

Currently Google is again before the European Court of Justice, seeking to win a case against a French data protection authority. The data protection authority argues with the support of both the French and Austrian governments, that the right to be forgotten should apply worldwide. Google is joined by various media companies to combat this approach, and the decision will undoubtedly have significant implications for search engines and social media giants including Facebook, Google, Yahoo, and Twitter. The issue poses tough questions for how to balance individual rights to privacy, with the public right to information.

Professors Jane Roberta Bambauer, and Meg Leta Jones, join us to discuss and debate this controversial issue, and predict what it may mean for global corporations moving forward.

Featuring:

Prof. Meg Leta Jones, Assistant Professor of Communication, Culture & Technology, Georgetown University

Prof. Jane Bambauer, Professor of Law, James E Rogers College of Law, University of Arizona

Teleforum calls are open to all dues paying members of the Federalist Society. To become a member, sign up [here](#). As a member, you should receive email announcements of upcoming Teleforum calls which contain the conference call phone number. If you are not receiving those email announcements, please contact us at 202-822-8138.

Event Transcript

Operator: Welcome to The Federalist Society's Practice Group Podcast. The following podcast, hosted by The Federalist Society's Corporations, Securities & Antitrust Practice Group, was recorded on Friday, October 5, 2018 during a live teleforum conference call held exclusively for Federalist Society members.

Wesley Hodges: Welcome to The Federalist Society's teleforum conference call. This afternoon's topic is the "Right to be Forgotten on the Internet." My name is Wesley Hodges, and I'm the Associate Director of Practice Groups at The Federalist Society.

As always, please note that all expressions of opinion are those of the experts on today's call.

Today we are very fortunate to have with us Professor Meg Leta Jones, who is Assistant Professor of Communication, Culture & Technology at Georgetown University. Also with us is Professor Jane Bambauer, who is Professor of Law, James E Rogers College of Law, University of Arizona. After our speakers give their

remarks today, we will move to an audience Q&A, so please keep in mind what questions you have for this subject or one of our speakers. Thank you very much for speaking with us. Professor Jones, I believe the floor is yours to begin.

Prof. Meg Leta Jones: Okay, great. Hi, everyone. What I'm going to do is introduce the "right to be forgotten" as it was introduced to the world as a global data protection right about eight years ago. Then I'm going to move backwards and talk about how the "right" is actually quite old in Europe, talk about how it has some American roots, and I'll introduce a little bit of terminology that might help us with the conversation over the hour, and then talk about the most recent things like the European Court of Justice ruling from 2014, the GDPR, and action that is happening here in the U.S.

So the "right to be forgotten" was presented to a global audience in 2010 when the European Commission announced its plans to update the Data Protection Directive from 1995 to account for major changes in information practices over the 25 years that had followed it. And in that announcement, they explained that the "right to be forgotten" was going to be on the table. American commenters, as you probably noticed, were quite critical and dismissive. They argued that it would be an exercise in, quote, "editing history" and would violate the integrity of the internet. At the time, it wasn't clear—it still isn't but at the time it definitely wasn't clear—what the "right to be forgotten" meant, but it was clear that it was intended to soothe anxiety about what was marketed as permanent online information.

People were worried about that their kids would do something stupid online and would forever be unemployable and have to live in their basement and thanks their stars that the internet didn't exist when they were young. Many were keen to debate whether people should be judged by content that they themselves put online, judged by content that other people put online about them, and people were generally -- or are generally and were generally worried about data collection that happened across sites in a way that wasn't clear and happened in quite a complex manner.

So the "right to be forgotten" is about deleting or creating barriers to discover ability for personal information that prevents an individual from moving on with their past or worried that this role will keep people stuck at the worst parts of their lives. So this seemed very new to us. I, as an American, was not familiar with this when I started studying it, but it's quite old. Not a lot of Europeans spent much time thinking about it either, but they do have much more experience with it than Americans do.

The "right to be forgotten" existed as a privacy right in many European countries and was used to help reintegrate individuals back into society after they had been sentenced or served time for a crime. The "right" prevented others from referencing the individual in relation to those prior crimes. So news could be edited, documentaries could be edited—and they were. It also existed as a data protection right. And these are two distinct ideas in European law, which is different than in the U.S. and causes a lot of conflation and confusion.

Most of the data protection regimes, the first wave that happened in the 1970s and 1980s, included a right to delete or a right to erasure of some kind. The bargain being that these powerful entities that were, at the time, using mainframe computers could utilize these technologies if they needed to be really transparent and allow for the individual to -- well, they need to be at least transparent and have some procedures in place to ensure accuracy and, worst case scenario, deletion. So these deletion rights existed in some places sometimes and not everywhere, not all the time.

The U.S., of course, has a little bit of history with this idea of redemption and rehabilitation, not so much in the data protection arena, though we do have aspects of the Fair Credit Reporting Act that suggest people should not be held accountable for their data forever, at least in a credit context. But even these court cases that are happening in the early half of the 20th century, we have cases that conflict with those. So I'm sure most people on the call are familiar with *Sidis [v. F-R Publishing Corporation]*, which is about the child prodigy that sued the *New York Times* when they published a "where are they now?" story about him. He unsuccessfully sued

them. And for the most part, the second half of the 20th Century is not friendly to this idea, that the individual's attempt or success at reinvention should override the public's right to know or an unfettered press.

So we also have this maximum floor set: equity will not enjoin libel. Meaning that even if we could successfully make some right-to-be-forgotten claim, we don't have a good tradition of deletion or erasure of information.

So I have talked about data protection versus privacy. One of the ways that I think is really helpful to talk about this—it's not entirely helpful, but it's a little bit helpful—is to think about the difference between data and content. So I refer to data as the bits that are passively generated and collected as users move through monitored spaces like websites and apps, and increasingly physical environments like shops and lobbies, airports. This is data that Europeans would call -- that's held by what Europeans would call the data controller. They process it, trade it, use it to better their polls, create new sources of information or revenue. They also have content, which is information about individuals that they themselves post or consume, and this may be posted by them or may be posted by somebody else in, presumably, some type of public publication. So this might be a Facebook post, might be a blog post, might be a YouTube video, an online news article, revenge porn—this is information that is actively produced and put out into the world.

So the "right to be forgotten" can address both or either of them. The European version addresses both and it does have exceptions for the freedom of speech and a research exception. It has a number of exceptions; I think those are the most relevant. The goal of each is to write some control over personal information having recognized the difficulty, to put it lightly, with managing individual data upfront. So a "right to be forgotten" offers a kind of retroactive form of control.

So the European Union Court of Justice established the "right to be forgotten" actually before the final version of the General Data Protection Rights -- or, I'm sorry, the General Data Protection Regulation, which just went into force in the spring, and

I'm sure you noticed all of the emails and the cookie banners that popped up. That was GDPR. And it includes a codified version of the "right to be forgotten" in Article 17. But the European Union Court of Justice established it based on the old Data Protection Directive from 1995 and the right to access and rectification article, which is Article 12 and the right to object, which is Article 14.

So the Court was able to find this "right to be forgotten" in a case that was asking it to determine whether an individual could force Google to edit the search results that came back when an individual searched his name. He was successful in that claim, and the Court came up with a way to kind of talk about the "right to be forgotten." It has been criticized, but if it links -- pointed to information that were—these are kind of the magic words—inaccurate, irrelevant, inadequate, or excessive, then the user had a right to its removal from the search engine. So there have been millions and millions of requests. I was just looking up the -- on the Google Transparency page, the numbers, and I will pull them up so I have them in a second. But it's a lot of information that has been removed, but it's only been removed in a sense that when you search for the individual's name, it doesn't retrieve results. So it is limited in that way.

Like I said, the GDPR codifies this in Article 17 as well as those exceptions. The debate today is really about whether the hurdle for discoverability that the "right to be forgotten" puts in place should be applied globally or only within a specific jurisdiction like the EU. I also want to flag, really quickly, that the new California Consumer Privacy Law that has sort of forced the hands of the federal government to consider federal privacy legislation for consumers includes a right to have businesses delete personal information that they hold. And there's also a number of kind of funny oddball cases that have occurred at the state level, and many of them have to do with criminal records, usually for people who were never prosecuted.

So I will leave it there, just teeing up some of the most current issues and kick it over to Professor Bambauer to explain all of the complications with this.

Prof. Jane Bambauer: Thank you, Meg. I'm going to focus most of my remarks on the -
- less on the data protection issue related to data that's collective passively, as Meg
put it, and more on the deletion of, or the obscuration of information that had been, at
least at one point, publicly available.

So the big debate about the "right to be forgotten," actually even putting it into a
larger context than that "right" itself, is whether we want people to have kind of an
ownership interest in other people's perceptions of them or not. And there're
alternatives that don't shift from an ownership model all the way to some sort of free-
for-all. We could have a risk-based or harm-based approach. But something like the
"right to be forgotten" puts people who are being described in websites in control of
that information to some extent. Obviously, the "right" is not absolute, and the
Google Spain opinion itself required Google and data protection authorities to do a
sort of balancing between those -- the interests of the subject of the speech and then
the public interest in the speech and having access to the speech.

But this ownership model, the control model, is really anathema to modern free
speech American law, as Meg mentioned, although there were some early privacy
cases that had thought about creating some kind of a limited right to a sort of
information redemption where you can require even traditional media to remove
information about past criminal records, for example. Those old cases have been
thoroughly rebuked at this point.

So in 2000, Eugene Volokh wrote an article for the *Stanford Law Review* that was
called "Freedom of Speech and Information Privacy: The Troubling Implications of a
Right to Stop People from Speaking About You." So that sort of represents, I think,
the traditional American vision that is brought to the debate about the "right to be
forgotten." But I could imagine an article written across the Atlantic that says, that's
called something like "Freedom of Speech and Information Privacy: The Troubling
Implications of a Loss of Control Over People Speaking About You," and that could
have just as much salience and meaning to a large swath of people.

The tension between these interests—access to information on one hand and controlling what people, especially misperceptions that people might have about you—is quite difficult to resolve. And before I go into -- launch into my long list of reasons that I think that the "right to be forgotten" is not a good idea, let me just acknowledge that it's completely foreseeable on the internet that there will be mischaracterizations about people and that sometimes this will be inaccurate information. But I think the more interesting cases are when there is accurate information that is nevertheless likely to lead to some kind of misperception either because of incompleteness of the information or maybe because of foreseeable overreactions that people would have to a piece of information. So I acknowledge that there is a risk or a harm that this "right to be forgotten" is trying to get at. But putting individuals in control of that problem is not the right solution.

So I wanted to first give you a sense of what Google is doing after the *Google Spain v. Gonzalez* case. Meg mentioned that these numbers are quite staggering, and they are. There have been requests to delist 2.8 million websites at this point, and about 20 percent of those websites are newspaper, news websites. Another 12 percent are social media, which kind of gets right to Eugene Volokh's article. That's where other people are talking about you to your friends or to their friends. And only about 1 to 3 percent—it was actually a little hard to figure out where in between those two statistics the real number lies—but about 1 to 3 percent of the requests involve what would be -- what at least Google would consider 'sensitive personal information,' which gets more protection under European law. And of those requests to remove sensitive personal information, 97 percent of the requests, at least 97 percent, are delisted. So the bulk of what we're talking about involve personal information that is not something like the identity of a rape victim or medical records or something like that.

About 6 percent of the requests to delist involve past crimes or past criminal procedures, and about 6 percent relate to professional misconduct. Most of the requests are rejected, about 56 percent are rejected because Google when it does its

own sort of independent assessment balancing the public interest and access against this interest in removing irrelevant or excessive information find that the public interest still wins out.

Google provides a little bit of information about how they make these decisions. They say, "We may determine that a page contains information which is strongly in the public interest. Determining whether content is in the public interest is complex and may mean considering many diverse factors, including - but not limited to - whether the content relates to the requester's professional life, past crime, political office, position in public life, or whether the content is self-authored content, consists of government documents or is journalistic in nature." But none of these factors are determinative and these factors don't necessarily push in the same way either.

But the important thing from this message, though, is that it's a rather -- despite the fact that Google rejects most requests, the standard that they are applying seems to be low in the sense that they find a public -- that they find the information to be relevant only if it's in the general public's interest or related to professional or political/public life. And so much of modern life and so much of modern use of the internet, in fact, involves little private decisions. And so one concern I'm going to raise in my remarks is just that it's a bit old-fashioned to weigh a person's private personal interest in controlling what other -- what their sort of small network of friends might think about them or small network of acquaintances and then weigh that against a large general public interest and access to the information, which usually will not be met.

So relevance and inadequacy, excessiveness—these are the terms that trouble me the most. The *Google Spain* case itself involves a Spanish citizen who wanted to remove reference to past debts that were old. And so I think the theory of the case is that somebody who sees references to these debts today would get the wrong idea about him and think that he's risky, a risky credit risk or just a sort of bad person, when, in fact, he may have moved on and changed the way he manages his own personal debts. So that takes a pretty strong position on what a person is judging this Spanish subject on, you know, what kind of decision they're making. And then, also, it

assumes that they will have bad judgment; that they won't see the context, that the judgment against them or that the debt was old - the unpaid debt was old, and that they wouldn't adjust; that basically that they would overreact to the information. And that sort of holds static. The misperceptions that may, in fact, happen today but could, with learning, change tomorrow so that we have a better understanding of how to weigh information.

And so I guess one of my biggest problems with the "right to be forgotten" is that it doesn't allow a dynamic process where, yes, there are potential victims today whose information will be misunderstood, where there will be misjudgments against them, but through that experience and through all of us having past skeletons in the closet exposed, we can learn to actually create a more fitting assessment of each other and of ourselves as well. So using, if I could change or butcher, I guess, a famous line by Lewis Brandeis in his famous concurring opinion in *Whitney v. California*, he said that "the fitting remedy for evil counsels is good ones," meaning that if there is information that's wrong out there, that the best approach is to add more information so that we can learn from it. That is, I think even I would admit, although I hope that that's true in the long run, and although I think that the First Amendment should continue to have that kind of aspiration, maybe a better, more modest goal that still gets us to the same policy end is that a fitting remedy for misjudgment at a certain time is to modify or change our expectations. And that, too, benefits from more -- generally speaking, it benefits from more information rather than less.

And Meg and I, we both think that there is a need for redemption from unfair human judgment. So I think the big question is whether left to their own devices, if Google or Facebook, through their voluntary actions, would do a good-enough job and leave the rest of us to sort of learn how to better calibrate our judgments against each other. Or if instead the imperfections that come through removing information through a government-imposed "right to be forgotten" would do a better job. So this is all -- this really requires a marginal analysis and requires, to some extent -- we're working off

of very little empirical information. So a lot of this winds up sort of tapping into our sense or philosophies about how humans react and how they behave and whether they're capable of change over time.

One last thing that gets a lot of attention when the "right to be forgotten" is raised is its capacity to help -- to sort of have the worst effects of attracting people who are trying to exploit a "right to be forgotten" in order to remove information that is not inaccurate and is, in fact, quite relevant. And so Google does provide some examples of instances where people have requested that information be removed when, in fact, it's related to their professional life. And so people who might be Googling them in order to understand whether they should contract with this person or become this person's patient or client really ought to have information about past misconduct.

One of the more striking examples came from Austria. Google said, "We received a request from the Austrian Data Protection Authority on behalf of an Austrian businessman and former politician to delist 22 URLs, including reputable news sources and a government record from Google Search. The outcome," they said, "is that we did not delist the URLs given his former status as a public figure, his position of prominence in his current profession, and the nature of the URLs in question." What's really troubling about this is that this person, who clearly has political connections, got the Austrian Data Protection Authority itself to make the case to Google. And so that's quite a bit of pressure being applied to remove what is very likely to be relevant information. Obviously, I don't know who this individual is or what the information is.

And then thinking about the Judge Kavanaugh hearings that have been going on, it, too, reminds me that something, some piece of information like a calendar from 1982 that seems so irrelevant today but could have explosive or very important meaning tomorrow is the sort of -- that's precisely the sort of information that a bad actor might want to cover up something that seems trivial or old or irrelevant, but in a specific known context—and I'm not talking -- actually, Kavanaugh involved a public hearing and a very public official—but in everybody's private life, something like this

could happen. You know, the Spanish man who brought his case against Google Spain to the European Court of Justice, for all we know there was somebody who -- you know, he had actually misrepresented his past credit history to somebody, maybe even not a creditor but a spouse or something like that, someone who may have just some unknown reason to want to get to the bottom of whether this person is truthful or whether this person is trustworthy in some way that Google and courts couldn't possible assess.

So the sort of impossibility of knowing whether a specific search result is relevant to a legitimate purpose that the search user has is -- it's a fiction. We don't know, Google can't know, nobody can really know whether information is truly relevant or not. What we do know or what we can predict is that, yes, some people will have some information that isn't properly calibrated or put in context because there's other missing information that doesn't show that they have redeemed themselves or something like that. But we also know that a "right to be forgotten" will be exploited by some people who are doing what Judge Posner had worried about a long time in his famous article about the right to privacy, where he predicted that the right to privacy might be used as a means to promote just personal fraud or social fraud.

So I think I'll leave it there, and, Meg, if you want to respond to anything I've said, please do.

Wesley Hodges: Professor Jones, I turn the mic back to you.

Prof. Meg Leta Jones: I would only respond to a couple of points, and I'll just do it really briefly because I love Q&A on this topic. I think one of the few places that Jane and I do disagree is—and I don't think I realized this until her comments—is the role of the DPA. One of the things that I found frustrating about the case and the way that the "right to be forgotten" has gotten structured in the EU is it eliminates the people that we elect or that are appointed through a democratic process. People go directly to Google. Google has this mysterious way that they decide these requests and weirdly, like Jane said, 56 percent of them are rejected. I have looked at this

almost every week for probably four years. It's always 44 percent; it's weirdly always 44 percent that they will take down, and I don't understand why and I never will, probably. So I prefer a system where individuals go to their local authority; they go through their own process and we argue about comity at a higher level and whether Google should be forced to do this, whether it violates First Amendment laws and the Speech Act. So this relationship that they've created really doesn't generate a good record for us to go off of.

And I will just lastly say that there's a weird framing that happens, and I think that Jane mentioned this in a way that we have to kind of reconsider what we see on the internet and how we judge people. I am a member of one -- well, of the most risk-adverse generations that we've had on record, except Generation Z is supposedly even worse than mine. And a huge part of that is attributed to the internet and this demand of perfection. And so, while this maybe isn't the law's role to play, I do worry that this is what we teach kids, is that if something ends up online, whether it's their fault or not, that it is dire -- you know, there're Disney PSAs that go out that tell kids that what's on the internet is there forever. They star *Phineas and Ferb* and there're called the Internet Rules of the Road. So that's something that I do feel like does really infringe on the autonomy and liberty of a mindset of an entire generation. So, yes, I will kick it out to questions now.

Wesley Hodges: Excellent. Well, thank you very much for that response. We do have one question in the queue, so Professors, let's go ahead and move to our first caller.

Mary Maxwell: Hello. It's Mary Maxwell from New Hampshire. This may be the last thing you'd expect a law-minded person to say, but I think you're omitting persons' right to be fraudulent about themselves. You just mentioned the [inaudible 28.40] article, and I haven't seen it, and naturally, you would take a law position against the right to fraud. But everyone's presentation of who they are to the whole world, especially those close by, it is their creation. I'm not saying right or wrong. I'm saying that it is normal. And I noticed that the two speakers are fairly young but in my day,

it's expected that everyone is always trying to up his image. And, of course, gossip is also an important guide against that or challenge against it because someone can lie about you or tell the truth about you.

But if you are only speaking in the context of what Google is saying, if Google is all very new with providing data that the person himself would not normally have provided to anyone, with private stuff like credit history, and that whole world of what is now available is all very new. So anything that would come about in jurisprudence now is radically different from what was possible before because things just weren't there. I don't really have a question other than to say -- to give you my two cents about the normalcy of being, pardon the word, fraudulent about oneself. We are always, always somewhat fraudulent about our presentation.

Prof. Jane Bambauer: This is Jane Bambauer. I'll respond. That's absolutely correct. Everybody is managing their reputation and perception at all times, and, in fact, we're doing it differently to different audiences. And so I agree with you descriptively. But also a historical fact is that we've never had, although we've tried to control other people's perceptions, we've never been able to, in fact, control what others can hear from third parties about us or we've never been able to remove gossip or control it to some -- to really any extent. But I agree with your point that with the new technology, it really pushes us to consider whether the theories we had about sort of, oh, gossip laissez-faire, for example, just letting people access whatever information they want about everybody else, whether that was based on presumptions, or at least assumptions, that were latent and that we never really bothered to examine carefully because we didn't have to because there was some limit to how much gossip could affect your life.

So there I agree with you, but that just raises the sort of salience of these foundational, theoretical questions of how much control we should or should not have over the information that other people get in order to try to have a non-managed assessment of a subject of a person. But it doesn't answer the question.

Wesley Hodges: Thank you, Professor. Let's go ahead and move now to our second caller of the day.

Evan Bolick: Hi, yes, this is Evan Bolick from the Rose Law Group in Scottsdale, Arizona. I do a fair amount of defamation work, which, as you can imagine, is mainly online. So in my opinion, Google and the other search engine's policies make it virtually impossible to take down speech that isn't constitutionally protected like defamation. But now in Europe, it sounds like there's a complete opposite problem where there's far too much speech being regulated and too many burdens on companies like Google to be taken down. Do you see any trend where we'll ever have a balance stricken between censorship and allowing for speech being taken down? Or are there any groups proposing to make it easier for removal of defamatory speech online?

Prof. Meg Leta Jones: I can jump in on that one. So I am hopeful that we will all come to our senses across a number of topics. The defamation question is great, and one of the things that's so interesting about the "right to be forgotten" is that it's about truthful information. And one of the clear distinctions between the EU and the U.S. is that the U.S. has, somewhat recently, explicitly questioned whether even lies have no value, of course, separately from defamatory lies, which is far and away different than countries that prevent people from saying -- that have laws for holocaust denialism, that prevent holocaust denialism from being mentioned without punishment.

So the question about removal I think is happening at the state level. That maxim that I mentioned, I'm sure that you are up against all the time, and my understanding is that in most defamation cases that involve the internet, the main ask is really removal; that would be wonderful. And there is a professor who did a survey of these cases. It's a little bit old now; it's from 2013. And his name is David Ardia from North Carolina, and he did find an increasing number of state judges who were forcing content or

forcing defendants to remove content based on a plaintiff's claim of defamation. So not this category of truthful information that we're talking about with the "right to be forgotten." But at least according to that article, there is a trend in that possibility.

Prof. Jane Bambauer: So I think that there are -- right, the route to have content removed from the website that is hosting it seems to be relatively well-established in law, although, of course, it requires some costs of various sorts for a plaintiff to go through those processes. But it's less clear what Google should do, even when it's handed an order showing that a plaintiff got some sort of judgment finding that—usually their default judgment finding—that some piece of content is defamatory. Precisely because they're often default judgment, Google does not know whether the information is, in fact, false because there was no interested -- there was no party that was apparently interested enough to actually defend the lawsuit.

And more troublingly in a case called *Hassell v. Bird* in California, Eugene Volokh—although I've already mentioned him once before—he actually had done a study with some attorneys, if I remember right, finding that many of the default judgments that were passed along to Google were actually fraudulent themselves, that they were against fake defendants so that they were designed to make sure that nobody would show up to court to defend keeping the speech online. And so that puts Google yet a different but another tricky position where it has to decide what to do when facing a, even what looks like to be a legitimate judgment from a state court that might have been kind of ginned up. So I imagine that problem might be affecting your practice.

Wesley Hodges: Thank you very much, caller. Let's go ahead and move to our next question.

Eric Lipman: Hi, this is Eric Lipman. I'm a judge in Minnesota and was hoping I could have our presenters weigh in on a question that's presented to my tribunal with some frequency. So in a case against regulated party act, Witness Y is called to the stand, and the judge makes a credibility determination saying that Witness Y when they testified, you know, it's not believable. It's not a credible witness when rendering

testimony. That, as part of the findings of fact, is dutifully recorded in the judge's opinion and is promptly, at the end of the case, posted online. And in the age of Google full-text word searches on particular names, frequently the witness, who wasn't a party against any kind of regulatory discipline or judgment, was entered, has a neutral state official saying, "I didn't find them believable," and that might impact business opportunities or employment. And we get requests saying, "Please take this credibility determination that I wasn't believable down from your website." There's a state-public records act answer to that, but I'm hoping maybe in a broader context, the presenters could discuss what they regard as the equities of -- not people who were directly involved in the litigation, but whose testimony is commented upon and are third parties or other hangers on.

Prof. Jane Bambauer: Wow, that's a tricky one. You know, I think one important aspect of the "right to be forgotten," for me at least, that it is government-mandated; the government requires Google, or whatever internet company, to at least consider requests to remove information. So in your case -- the reason I say that is in your case where you're commenting in a closed-system—of course, your court is also a state actor, the government—but where you're commenting on this closed system where you're trying to do your best to assess credibility and you know -- I'm sure that you and many judges have an admiral amount of humility and understand that you have limited time and resources and information, and you're making these credibility judgments that are the best you can do under the circumstances but are not necessarily completely accurate, it may make -- I mean, I would say that may be a context where as a default, at least, that kind of public record should be redacted -- the names could be redacted and at least I think there's a theory that would explain why that would make sense. Meg?

Prof. Meg Leta Jones: Yeah, I absolutely agree. That is an awesome question, by the way. That's the perfect kind of issue. And as a researcher that regularly is digging through public records, following employer requests, it's -- everything doesn't need to be immediately in a Google-searchable form. I think that we can resist the urge to internet-ify everything. Everything doesn't need to be connected. And I think this is a

great example of when we can take at least the collateral damage of privacy issues where we're talking about collateral damage and we can say, "Hey, we're not destroying this record by any stretch of the imagination. It's there. We have laws in place that make sure that record will always be accessible through appropriate channels." But what's limiting this person's life is that anyone can just put their name into a Google Search spot, which is what everyone does, and this required service that they provided generates a negative response to searchers.

So I would say that that is another instance where using all of our digital tools is a great idea so you can apply a robot.txt file to that particular file and you can do this -- you can create a text file that signals to search engines not to crawl certain pages. That can help if you want to maintain them in their full state. You could redact them just like Jane said. You can, especially I think if you do something like that, stating what your policy is so that people know that they need to go an extra step, that that's what it takes to find this public information. --

Prof. Jane Bambauer: Yeah, if you don't mind I'll add one more thought I had that Meg reminded me of, that there are some contexts where you can preserve much of the utility of the information that might be -- that you might want to put online or that you, through public records law, must put online, while removing those things that are the most potentially riskier or hazardous or harmful. So I would think -- I would err of the side of redacting names rather than telling Google not to crawl a page, especially if it's a full opinion, at all because the rest of the context might be very useful, very relevant to some legitimate public access. Whereas the name of this one particular witness is not particularly useful except for somebody who's just trying to understand that particular person more. And then for that searcher, this one pronouncement by you might not be very good or useful information.

In a larger sense -- but I came to this topic in my research because I used to do data-driven research using public records. And so I'm very sensitive to trying to keep the utility of records without causing too many privacy harms. And I think a lot of times we miss -- the understanding tends to come in black and white form, where either a

record needs to be fully public for all purposes or really obscured to the point of not really being freely available at all. And if there're certain types of information, like names, that could just be redacted and still preserve most of the value, I hope we go in that direction instead.

Wesley Hodges: Thank you so much, caller.

Jane Robbins: Hello. My name is Jane Robbins. I'm from Georgia. And this may open up another area that is beyond what we're talking about, but I am concerned about all of the data that is collected on children in Pre-K through 12th school through the technology. And, of course, Google gives all of this, quote, "free" stuff to schools so that they can get the data. And then the companies, not only Google, but hundreds of others will use this data for commercial purposes and to create predictive algorithms about students, and it's widely swapped on the net with data brokers. And obviously the students don't know what's being collected and neither do the parents. And so my question is about the possibility of having an ability for parents to demand that that data be erased at the end of a course or at the end of a school year. I'm interested in your comments about that.

Prof. Meg Leta Jones: I have some comments about that, also. I have a similar gripe. I really like technology in schools to begin with. So we're using -- forcing students to utilize a lot of different platforms, I think is frustrating. And you're right, they usually are like a Google Suite or a Microsoft Suite whatever the contract is with the school. There are laws that we have in place for kind of at two different angles of that. FERPA is the student data privacy law that we have and that covers educational institutions, any that takes federal money from the Department of Education, which is just about everybody. And they do have to adhere to very different information practices as business partners, and I may be butchering new legal terms on [inaudible 44.57] crept on student privacy. But they do have to have different -- they do have different information practices for student's data than everybody else's data that uses Google.

And then there's also COPPA which is celebrating, I think, its 25th year. And that is the Child's Online Privacy Protection Act. So beyond the school district there's additional layers of protection and really control that's granted to parents. So there's all of these means that are supposed to be provided to parents to help them manage their children's data, including retroactively. The fact that you have not been presented with either of these, I think shows that we aren't great at integrating those privacy laws and privacy practices into our daily use for kids. Jane, do you have anything to add to that?

Prof. Jane Bambauer: Well, I had one question for you. I didn't know that either of the laws offer retroactive relief. I thought both require consent for certain uses and certain collections, but that -- I was not aware that either of them would allow a parent to revoke consent later.

Prof. Meg Leta Jones: So I don't know about FERPA. I thought that COPPA did. But you're right. I don't know. So that's a good question. But that's where you would look for the answer to that question.

Jane Robbins: If I could bring up something else. FERPA, of course, applies only to educational records, and there's a real question about whether the kind of data that's collected by all of these engines that shouldn't be there to start with actually qualifies as an education record. The other problem with FERPA is that the Obama administration gutted it in 2012 by regulation. And so FERPA essentially protects almost nothing. As far as COPPA is concerned, there are reports, studies that have been done showing widespread -- just ignoring COPPA when it comes to software that's used in schools. Plus, COPPA only applies up to age 13, so that leaves kids in high school with the same problem.

Prof. Jane Bambauer: Stepping back a bit, even if the laws on the books could be better enforced, I think another question is whether we should have some kind of a right to erasure that either parents or students later in life can activate. And this kind of -- you're forcing us, I think, to recognize that maybe the distinction between the

publicly available information that we were focusing on with the Google "right to be forgotten," the *Google Spain* decision, and then the GDPR or data privacy issue is really not as distinct as maybe it initially seems because my guess is that Meg and I would have largely the same sort of set of pessimistic or optimistic predictions about the data privacy or data collection issues that we do about the publicly available information. And so, yeah, I would worry that to the extent that these platforms are creating cheap and effective educational tools and to the extent that the data that they're collecting either helps them improve those tools or helps them finance them, I would worry about a strong consent model or even an inalienable right to remove data because, at least if it's used frequently, it could undermine whatever value that we're getting.

So I think there's a big question of whether there's enough value added. Assuming that there is and assuming that these tech companies are filling some needs in public education, I would want to be careful before giving anybody the power to kind of sort of kill the technology.

Prof. Meg Leta Jones: Jane, can I ask you a question? Sorry, I'm not in the queue. I haven't pushed the star button, but can you explain just a little bit more what you mean by strong consent model in this context? You said you would be hesitant about a strong consent model.

Prof. Jane Bambauer: So a strong consent model -- by the way, Meg, I read your TPRC paper and so I think consent's been on my mind. A strong consent model means, I mean, it's basically where -- certainly where California has gone and where the U.S. is, to some extent, headed in the European footsteps. But a strong consent model basically says that consumers have kind of overwhelming interest in understanding how their data is collected and used, and should be given not only clear notice, very effective notice—or you know, not just in a long end-user contract but effective notice, just-in-time notice—and then an opportunity to reject the terms and yet still use the service—at least that's to some extent suggested in the California law; it's not clear it's going to be enforced that way. And then the GDPR is very clear

that these companies need to provide the service even though they're not having -- even though they may not be able to process data the way that the service had intended or expected to be able to.

So that form of consent, I mean it basically creates more than a property right, depending on whether the company has to continue to provide service even without accessing data. But at the very least it's a sort of property right that information about me is mine, and therefore you can't take it, you can't copy it, share it, use it unless you have consent from me. That's what I mean.

Wesley Hodges: Excellent. Well, it looks like we're at the top of our hour now. Thank you to everyone for your questions. Professors, do you have any final remarks you'd like to make before we wrap up today?

Prof. Meg Leta Jones: My last remark would be to mention one point that hasn't come up which is that the internet is very not permanent. Things fall off the internet all the time. Our bigger problem probably than the "right to be forgotten" is digital decay and link rot. And so it's a related topic, but another giant issue.

Prof. Jane Bambauer: I think I've said enough, so thank you very much.

Wesley Hodges: Wonderful. Well, thank you both so much. On behalf of The Federalist Society, I'd like to thank you for the benefit your valuable time and expertise. We welcome all listener feedback by email at info@fedsoc.org. Thank you everyone for joining. This call is now adjourned.

Operator: Thank you for listening. We hope you enjoyed this practice group podcast. For materials related to this podcast and other Federalist Society multimedia, please visit The Federalist Society's website at fedsoc.org/multimedia.



Jane Bambauer



Meg Leta Jones