Pages 1 - 110

UNITED STATES DISTRICT COURT

NORTHERN DISTRICT OF CALIFORNIA

Before The Honorable Edward M. Chen, Judge

hiQ Labs, Inc.,	)	
	)	
Plaintiff,	)	
	)	
VS.	)	**NO. C 17-03301 EMC**
	)	
LinkedIn Corporation,	)	
	)	
Defendant.	)	
	)	

San Francisco, California
Thursday, July 27, 2017

TRANSCRIPT OF PROCEEDINGS

APPEARANCES:

For Plaintiff hiQ Labs, Inc.:
Farella, Braun & Martel LLP
Russ Building
235 Montgomery Street, 18th Floor
San Francisco, California 94104
(415) 954-4400
(415) 954-4480 (fax)
BY: DEEPAK GUPTA
CARL BRANDON WISOFF

Laurence H. Tribe
Carl M. Loeb University Professor and
Professor of Constitutional Law
Harvard Law School
1575 Massachusetts Avenue
Cambridge, MA 02138
(617) 495-1767
BY: LAURENCE H. TRIBE

Reported By: Lydia Zinn, CSR No. 9223, FCRR, Official Reporter

APPEARANCES:

For Defendant LinkedIn Corporation:

Munger Tolles & Olson LLP
1155 F Street NW, 7th Floor
Washington, DC 20004
(202) 220-1101
(202) 220-2300 (fax)
BY: DONALD B. VERRILLI, JR.

Munger, Tolles & Olson, LLP
560 Mission Street, 27th Floor
San Francisco, CA 94105-2907
(415) 512-4009
(415) 644-6909 (fax)
BY: JONATHAN HUGH BLAVIN
ROSEMARIE T. RING

Thursday - July 27, 2017 **1:57 p.m.**

P R O C E E D I N G S

---000---

THE CLERK: Calling Case C. 17-3301, hiQ Labs versus LinkedIn. Counsel, please come to the podium and state your name for the record.

MR. WISOFF: Good afternoon, Your Honor. Brandon Wisoff, Farella Braun & Martell, on behalf of plaintiff, hiQ Labs.

THE COURT: All right. Thank you, Mr. Wisoff.

MR. TRIBE: Good afternoon, Your Honor. I'm Laurence Tribe, here for hiQ.

THE COURT: All right. Thank you, Mr. Tribe.

MR. GUPTA: Good afternoon, Your Honor. Deepak Gupta, here for hiQ Labs.

THE COURT: Thank you, Mr. Gupta.

MR. VERRILLI: Good afternoon, Your Honor. I'm Don Verrilli, from Munger Tolles Olson, for LinkedIn.

THE COURT: All right. Thank you, Mr. Verrilli.

MR. BLAVIN: Good afternoon, Your Honor. Jonathan Blavin, for LinkedIn, from Munger Tolles, as well.

THE COURT: All right. Good morning.

MS. RING: Good afternoon, Your Honor. Rosemarie Ring, Munger Tolles & Olson, also on behalf of LinkedIn.

THE COURT: All right. Welcome, everyone.

Okay. We are on, obviously, for hiQ's motion for preliminary injunction. This case, of course, raises a number of cutting-edge issues, but we are framed by a basic, well-known framework here with respect to the standard for preliminary injunction. And one of the first questions that's going to guide the analysis on the merits is the balance of hardships. And so I have to determine which way the balance of hardships tips; and if so, how sharply or not sharply they tip.

Now on the one hand, hiQ contends that it will be subject to bankruptcy, essentially. And maybe you can elucidate if there's any more information in that regard if the injunction does not issue here.

MR. GUPTA: Your Honor, the injury would be devastating. The company's been already in a bit of a tailspin. Before the cease-and-desist letters were sent there were 24 employees, and we're now down to 15. There was a resignation earlier this week. The momentum of the company is suffering over the uncertainty of this case hanging over its head, and we're living day to day as to whether basic raw materials of the business are going to be available to them.

THE COURT: And all of the raw materials are taken from LinkedIn? There's no other --

MR. GUPTA: Your Honor, the vast, vast preponderance of the public material they're using is from LinkedIn, because

of LinkedIn's tremendous market power in this area as the host of 500 million professional profiles for the world's professionals.

THE COURT: Well, there was reference to the fact that other similar companies doing analytics are able to work without using LinkedIn, but using other sources. What's your take on that?

MR. GUPTA: Your Honor, we talked with the client about that. And these other companies are doing something different. They're not doing what hiQ does. HiQ is in the data-science business. And all data-science companies dating back to Alta Vista and Excite and Google require data; and public data is what people use. That's the business hiQ is in.

These other companies do things like perform surveys on employees about their employee satisfaction. And that type of data -- while some of these companies may choose to make a business out of it, hiQ never opted to go in that direction. And I think there are good business reasons why they didn't go in that direction.

THE COURT: But aren't there -- who would you say would present databases about employees that, if one had to, besides LinkedIn, what other sources are there of data?

MR. GUPTA: Your Honor, our team has been looking into that question for -- for months now. And there are no

real alternatives to this data.

In LinkedIn's papers they suggested that Facebook might be an alternative source, but that doesn't really pass the red-face test, because everyone knows Facebook is a social-networking platform where people connect with their friends, post photographs, and that sort of thing. It's not a serious professional platform, where you can get skill information and the other types of data that hiQ works on.

THE COURT: You want to comment on that, Mr. Verilli; just that point?

MR. VERILLI: So, Your Honor, if you would like us to address that specific point, I'm going to ask my colleague, Mr. Blavin, to do so.

THE COURT: Sure.

MR. VERILLI: I do have some more general points I think are of real significance on the balance of --

THE COURT: Right. I haven't gotten to your side of the ledger yet.

MR. VERILLI: But in terms of that, maybe we'll have Mr. Blavin. Thank you.

THE COURT: All right. Mr. Blavin.

MR. BLAVIN: Thank you, Your Honor.

As Your Honor correctly identified, there are a number of other competitors in what's called "the people analytics space" that operate using alternative data inputs. One of them is the

company, Glint, which we highlighted in our papers, which uses internal surveys to collect data relating to employees. It is viewed as a direct competitor to the type of services that hiQ is offering.

THE COURT: But that's a very different process than -- I mean, you just said it's internal surveys, which is quite different than being able to sort of surf the World Wide Web for posted information.

MR. BLAVIN: It's different in the sense that it's getting a different type of data input, but the actual service it's offering within what's described as "the people analytics space" is remarkably similar. So if the question is, "Do other companies exist in this space, and do they offer competitive offerings, and succeed, without using scraped LinkedIn data," the answer to that question is "Yes."

Moreover, there are a number of other websites which do have professional data on them, including skills data, job descriptions, education, et cetera. We highlight in our declarations and in our brief a number of those, and one of them is Facebook.

And notwithstanding that hiQ just generally takes the position, *Well, that's not a professional network*, we've put forward evidence in the Blavin Declaration and other supporting declarations which show that Facebook has a substantial amount of professional data on it.

For example, one of the things that we did in our declaration is we looked at the advertising tools on Facebook and on LinkedIn, searching for people who describe themselves as working for a particular company. You can target ads to those people.

And the numbers of people as to various companies, including hiQ's own clients, who describe themselves as employees of those companies -- so they're obviously putting down who their employer is -- the numbers are remarkably close, between LinkedIn and Facebook.

And Facebook has the same fields that LinkedIn does that they're describing: Job titles, skills, education, job descriptions, et cetera.

Moreover, survey evidence which we put in showed that on Facebook, 74 percent of users put professional data on it, as compared to 78 percent of LinkedIn users. So notwithstanding the conclusory allegation that only LinkedIn has professional data, the actual evidence in the record demonstrates otherwise.

THE COURT: Okay. What's your response to that?

MR. GUPTA: Your Honor, the company has invested $14 million in a particular business.

What LinkedIn is suggesting -- and the hubris is astounding -- is that we should take that $14 million investment, write it off, and completely reinvent the business to either do employee internal surveys, or somehow figure out a

way to use Facebook to make a viable product.

We have client contracts today that are based on the product that we developed. We won the HR Product of the Year in 2016 for our Keeper product, because our product is extremely compelling.

They're saying, *Well, forget about that product, guys. Do something completely different*.

We're saying, *No. "Public" means "public."* We built a product on public information.

THE COURT: Well, what Mr. Blavin is referring to is not just the model of doing internal surveys -- I understand it's a completely different process -- but doing the same thing, running the same kind of analytics, but using a different database, which they say or he says has the same kind of information one would likely find in LinkedIn.

MR. GUPTA: Your Honor, if there were a solution like that, our client would have figured it out, because they have no desire to be paying our law firm this kind of money to be fighting against a powerhouse like Microsoft or LinkedIn.

The reality is Facebook may have a field in it where some people choose to put down the name of the business they work for. That's utterly worthless for the hiQ product. What the hiQ products depends on is a robust, complete description of a person's professional skills, previous employment, interests, that kind of stuff, and update it on a regular

basis, so that it is a very rich resource that they can then extract these analytics from.

Facebook is -- they've looked at it. We've talked about it. Facebook cannot hold a candle to LinkedIn as a professional networking site.

Your Honor, I think their own product marketing collateral tells the whole story, which is, *We have 500 million-plus members. We are the world's largest professional networking site*. That's their own words.

THE COURT: Is there anything in the record that suggests or describes a difference in the quality and the depth of the field of information, as a practical matter, that is available from Facebook vis-à-vis LinkedIn?

The fields may be available, but maybe people don't use it very often, because they maybe consider it more of a social as opposed to a professional network. The age, the demographics may be different, such that utilization may be different. Maybe the amount of attention in terms of updating is different. I don't know. Is there any data that actually compares these two, in terms of their richness of the data?

MR. GUPTA: Your Honor --

THE COURT: Professional data.

MR. GUPTA: Your Honor, if we had to piece something together from the Record, I think if you look at Exhibit E to their TRO papers, that shows what LinkedIn has. You know. And

I don't think they've put in the comparable profile from Facebook; but a Facebook profile does not have that kind of information in it.

Furthermore, I think if you look at the Mark Weideck Declaration, who's the CEO of our company, he states quite clearly that there's no other source. He had his CTO and his team working around the clock when they got the cease-and-desist letter, saying, *What do we do? You know, we're fighting for our lives here, guys*.

And these -- these engineers were working around the clock, trying to figure out a way: Well, can we somehow use a different source of public information? Is there anything out there? How do we keep this going?

It was only after they reached a conclusion that there is no alternative that they said we need to take this measure.

And we did try to talk with them. We did try to explain this to LinkedIn before we pursued this route. It was unfruitful. And that's why we ended up -- and that's why we're here today, where we are.

THE COURT: All right. Let's focus on the other side of the equation: Hardship --

MR. BLAVIN: Okay.

THE COURT: -- to LinkedIn if the injunction were granted. And I know part of this that you made a big part of your case has to do with the preferences in the more granular

settings -- display settings or privacy settings -- that have been opted for by LinkedIn users; namely, for instance, not broadcasting changes made to their profile, I guess, with the risk that that might be interpreted by their employer as job hunting, or something. So why don't you elaborate on that?

MR. VERILLI: Yes, exactly, Your Honor. Of course, we're focused on the balance of equities here, and I'm going to address that directly. To get to the balance of equities, they've got to show likelihood of success on the cause of action, or at least a serious question; but putting that to one side, because we think they're nowhere near that here -- but with respect to the balance of equities, what we would submit is the most important equity before this Court now -- the overriding equity -- are the privacy interest of LinkedIn's members, and the integrity of LinkedIn's trust relationship with its members, which is essential to its business.

Your Honor identified the Do Not Broadcast feature. And I think that's of critical importance. The second Rockwell Declaration, which is attached to our supplemental brief, details the facts on that. And our brief discussed it, too. And it's critical. Many millions of LinkedIn member, when they change their profile settings, have opted not to chose the Do Not Broadcast feature, which means that that information is not sent out to their contacts, and not send out to their employer. And so they've made that decision, as paragraph 4 of

the Rockwell Decision [sic] -- the Rockwell Declaration identifies, because we put that policy in place precisely because LinkedIn members were worried that when they made a change to their profile, that their employers might get notice, and be -- and be suspicious that they were searching for a new job. And that was an invasion of their privacy. And that's why we have it.

And of those many millions of LinkedIn members --

THE COURT: It was about 50 million, as I recall, that have opted in?

MR. VERILLI: That's correct, Your Honor.

THE COURT: Is that about 10 percent of the user base?

MR. VERILLI: Right, but I think in addition, well more than 10,000 of our members are employees of the companies with which hiQ already has contracts, so they're already under this surveillance, and they're already at risk of being ratted out to their employers with this system.

And so -- and that's a -- that is a very serious intrusion on their privacy. Basically what's happening here is that they have chosen -- our members have chosen Do Not Broadcast. And hiQ is broadcasting the very information to the employer that we have that our members have chosen not to broadcast.

Now even with respect to the other members who haven't chosen that option, they have made their data visible -- their

information visible on LinkedIn, on the basis of an understanding that we are going to respect the Terms and Conditions that we have communicated to them.

One of the Terms and Conditions we have communicated to them is that we don't allow scraping and data mining of this kind, because it is an intrusion on their privacy.

And, as Your Honor will see from the second Rockwell Declaration, we have also received numerous complaints from our members that they believe that this kind of an intrusion -- this kind of scraping, and data mining, and ratting them out to their employers, or disclosing this information in other ways -- is an invasion of their privacy; is incompatible with what they understood.

THE COURT: Now let me ask you. I'm trying to recall. When you say they've been informed that data, quote, "scraping" -- I'll say quotes, because some people find it is a loaded term, but I'm not sure what term to use for now. I know that's term that's used, because one of your arguments is that hiQ signed on to that, and they're bound by that.

But how explicit is it that this is not allowed, not only by users, but just generally; that LinkedIn takes affirmative steps to block third-party, quote, "scraping," even if they haven't signed this Agreement?

MR. VERILLI: Of course, they have signed --

THE COURT: Right, but --

MR. VERILLI: -- but in addition --

THE COURT: -- I'm talking about notice to the average user.

MR. VERILLI: Right. It's in the Privacy Policy, Your Honor. It's in the Privacy Policy, which is incorporated among the Terms of Use. And the Privacy Policy states more generally. It doesn't just state that if -- by agreeing to this User Agreement, you may not engage in scraping. The Privacy Policy more generally states that we have measures in place to protect your privacy in this way.

And it's the complaints that we have identified from our members in the Rockwell Declaration, some of which we've quoted in our brief, show Your Honor the members take that seriously. And they believe that their privacy is being violated by this.

THE COURT: Can you identify --

MR. VERILLI: And then --

THE COURT: -- where that Privacy Policy --

MR. VERRILLI: I don't have it at my fingertips, Your Honor, but we will find it.

And then, of course, in addition to that, you know, LinkedIn does maintain a vigorous set of technical measures, which are outlined in the first Rockwell Declaration, which are there to protect our members from -- and I'm going to use this term, because it's the term -- "scraping" by automated bots, which can be done for all kinds of purposes. It can be done

for identity theft. It can be done for other scams. It can be done for spamming.

And, as Your Honor is aware from the prior submissions in this case, those technical measures turn away 95 million incursions by automated bots every day. We have no way of knowing in advance which of those automated anonymous bots is seeking information for one purpose or another.

What we know is that all of them are acting in violation of our Terms of Service. All are acting in violation of our policies. And we need to protect our members' privacy interests against all of those kinds of intrusions, including hiQ's intrusion.

Now, that's a very powerful equity here, that -- when you think about that, yes, they've got a certain number of employees. Whether their business is at risk or not, I don't know; but if it's at risk, it's at risk because they have designed a system that -- and I realize we're moving a little bit to the merits here, but I will confine myself on that. But they've designed a system that, in our view, is unlawful.

And that -- in our view, they have not identified any legal basis that would require us to disable our technical measures so they can get access on the terms that they want access, which we don't give to the general public, and we don't give to others who want to scrape data for whatever purpose.

THE COURT: I think I asked this last time. Is there

any kind of a setting that's available to LinkedIn users who might want to be able to be out there for all purposes, including being subject to collection by bots, because perhaps there are some advantages to it? Some might think that there is. Is there an option to allow that?

MR. VERILLI: I'm not aware that there is. Mr. Blavin can correct me if I don't have that fact right. I'm not aware that there is; but I also can't imagine that there are very many members who are going to think something like their Keeper product is something they'd want to have themselves subjected to, which is -- it's essentially corporate intel. It's an anonymous surveillance of their behavior, to rat them out to their employers. And I can't imagine that any member would think that that would be something of benefit to them.

THE COURT: Well, I mean, hypothetically that was something posed initially by hiQ, is that people might be seen as valuable, as "keepers." They think they are going to be seen as keepers. And this is their subtle way of letting their employers know that there's free agency out there, and they might want to keep them.

MR. VERILLI: I guess my point in response to that, Your Honor, would be that that ought to be up to the autonomous choice of the members. It ought not to be up to hiQ, as a matter of making a buck.

THE COURT: Well, that's why I asked. If you wanted, really, a democratic process --

MR. VERILLI: Right, right.

THE COURT: -- one could envision that people could have that option.

MR. VERILLI: But I guess, Your Honor, what I would say is if somebody wants their employer to know that they are looking for a new job because they think it will give them leverage, they don't need hiQ to tell them. They have plenty of ways that they can convey that information.

You know, I think this Keeper product is all down side.

And then there's another equity here even with respect to the other product, which they try to portray as just something that has no negative effects, as an equitable matter, at all -- and that's completely wrong -- their Mapper product.

Well, a lot of people make a decision to make their profile visible, and then at some point in the future make a decision that they no longer want it to be visible, so they take it down; but at that point, hiQ's got it. And so it's not -- you know, so they have lost that control. They've lost that autonomy to decide what people know about them over time, because hiQ's taking that information, in violation of these norms on which we run our business, and they've got it permanently. And so there's -- that's another way in which there's a real intrusion on the --

THE COURT: Are there not other archival-type websites out there that store this information?

MR. VERILLI: I'm not aware that that would be available, Your Honor; but what I do know is that they take that -- that when members decide that they no longer want their information visible, that's a choice that hiQ effectively has overridden. It's overridden their privacy. It's overridden their autonomy. It's done it in numerous respects. It does it to hundreds of thousands of people, including tens of thousands of people who are employed by hiQ's clients.

And I think that that is an extremely powerful set of equities that far outweighs any equitable claim that hiQ has to try to run this commercial enterprise -- we believe, in violation of the law; certainly in violation of all of the policies that we set up to protect our members. And that doesn't even get -- that's just about the members.

You also have to, I think, Your Honor, consider our business model here. Our business model depends on a trust relationship between us and our members. We need to have our members put this information up and put it into the system and make it available, in order for our business model to work. And in order for that to happen, they have to trust that we're going to be able to do what we say we're going to do, in terms of protecting their privacy and protecting their autonomy.

And what hiQ comes in and says, essentially, is, *Doesn't*

matter. Does it matter what you tell your members about how you're going to protect their privacy. We get to take that information, and use it for whatever purpose we want.

And that is deeply damaging to our relationship -- the fundamental relationship that makes our business work.

THE COURT: Have there been any kind of surveys, other than a collection of complaints, whether by your client or anybody else, that look at what users' privacy expectations are, whether it be Facebook, LinkedIn, or anything else, when they choose a public setting?

Because one could make the argument that once somebody goes public -- and they have a range of options, whether it's Facebook or anything else -- they're taking a calculated risk. And they do that at their own risk, and perhaps knowing that there's a risk that -- who knows what kind of data? I mean, there are all sorts of people out there. Could be creditors, and all sorts of things. But if you put it out there, that's the risk, and that's what people expect.

MR. VERILLI: So a couple of points about that, Your Honor.

First, I think -- while I don't know the answer to the question whether there have been any kind of surveys with respect to that particular question, I think, based on this Record, by far the fairest inference is that LinkedIn's members put that information out there, when they make it visible, on

the understanding that the conditions that LinkedIn has imposed are going to be respected, and that therefore their privacy and their integrity is going to be respected.

And the second point I'd like to make -- I think this goes a bit to the merits. I think it's also highly relevant to the balance-of-hardships analysis that we're talking about here -- is that what I would submit to Your Honor is that, with all due respect, the dynamic is exactly the opposite. If it were the case that LinkedIn can't continue to use these technical measures to block the kind of scraping, and data analytics, and the ratting-out to the employer that their business model relies on -- if we can't do that, that's not going to increase the free flow information to the public.

It's going to decrease the free flow of information to the public because what's going to happen is that many, many more people are going to be unwilling to make their information visible, precisely because they're not going to want to take that risk. For example, that number of people who choose Do Not Broadcast, I'm sure, is going to go way, way up if this is permissible activity. And in addition, Your Honor, I'm sure that many, many fewer people are going to make that information visible, at all. That just stands to reason.

So I think the fact, Your Honor, it's not the case that people understand that they're taking a risk. They think they aren't taking this risk. And once they learn that they're

taking this kind of risk of being exposed to their employer, and having data that they no longer want public remain public -- they're going to make the decision not to make that data available in the first place.

And the only other option we have under their theory of the way the law is supposed to work: Either we've got to tell our members this, which is going to lead to that reduction in the free flow of information, or we have to put up a wall; something like -- keep the information inside a wall with a password, which, of course, is going to decrease the free flow of information, because you won't be able to get it if you're outside the wall.

So I think as an equitable matter as well as a legal matter, that that runs exactly in the other direction. What they're asking for damages our members' privacy, damages our business model, damages the free flow of information. It benefits them and their 20 employees, but it damages every everything else I've just listed in a very serious way.

And, of course, the problem, Your Honor, is if they can do it, so can everybody else. This isn't a hiQ-only pass. If they can do it, everybody can do it. And then I think you're talking about a very, very serious denigration of important interests.

My colleague, Mr. Blavin's, got the Privacy Policy site here, Your Honor, for you.

MR. BLAVIN: Yeah. So two things, Your Honor.

First, with respect to the User Agreement, we know that hiQ accepted and agreed to that. They don't dispute it. It's important in terms of member expectations, though.

The User Agreement says, in Section 1.1, that it applies to anyone who accesses or uses LinkedIn's services. And, as Your Honor is aware, in Section 8.2 it says if you're going to access our site, you have to -- you know, we've quoted this repeated times -- not use software, devices, scripts, robots, or any other means or processes to scrape the services.

So a member, reading the User Agreement, itself, would think that anyone who's accessing LinkedIn has to agree to its terms, which included an explicit anti-automated-scraping prohibition.

THE COURT: Does that make it clear that it applies to nonmembers?

MR. BLAVIN: Well, it applies to anyone. The Agreement says, *You agree that by clicking Join Now to join LinkedIn, to sign up, or similar, registering, accessing, or using our services, you are agreeing to enter into a legally binding contract with LinkedIn*. So it applies to those who simply access the site, as well.

THE COURT: Is there any statement in that policy that says, regardless of contract or membership, that we take steps to preclude scrapers, et cetera?

MR. BLAVIN: Well, as noted, it says that if you access the site, you can't scrape.

THE COURT: Yeah. I understand that, but is there something more affirmative that says, *We protect you, user, against these third parties who might want to scrape your data*?

MR. BLAVIN: Section 4.5 of the Privacy Policy, which is attached as Exhibit C to the first Rockwell Declaration, states that we have implemented security safeguards designed to protect the personal information that you provide, in accordance with industry standards.

It further goes on to note that to protect any data you store on our servers, we also regularly monitor our system for possible vulnerabilities and attacks. And we use a tier-one secured-access data center.

And the security measures are those that are outlined in the Rockwell Declaration to prevent the estimated 95 million automated attempts to access the site on a daily basis.

THE COURT: This is C?

MR. BLAVIN: Yeah. Rockwell Declaration.

THE COURT: Where would you say is the --

MR. BLAVIN: It's in Section 4.5, which is at the end of the Privacy Policy to the first Rockwell Declaration, not the supplemental one.

THE COURT: Well, this refers to information that is secure. It's stored. It's stuff that you secure bypass word,

and everything. We're taking measures to make sure that that's not hacked.

It doesn't say -- it does not -- I don't see anything here that suggests that things that you have set for public view is not going to be subject to aggregation, or some kind of analytic aggregation.

MR. BLAVIN: Well, it does say that *to protect any data you store on our servers*.

Data that is publicly visible on LinkedIn is data stored on our servers.

THE COURT: Yeah. I'm sure you can read it like a lawyer, but I don't think this says that.

And chances are 2 percent of the people reading this thing -- the 2 percent who do -- I bet you if you took a survey right now and asked, *Did you understand this to mean that you would not be subject to any kind of aggregative collection, with the exception of authorized search engines like Google, that you* --

I don't see that here, frankly.

MR. BLAVIN: You know, I respectfully push back, to say that those security measures are the ones that are detailed in the Rockwell Declaration.

THE COURT: All right.

MR. BLAVIN: Moreover, if there were a survey to say how many people would opt into the type of service that hiQ

is offering, given everything that Mr. Verilli stated before about the measures, the features, that LinkedIn has 50 million people locked into them, I think it would be a very, very low percentage that would actually opt into that type of service.

THE COURT: All right. Let me hear your response to particularly the concerns that they've raised now repeatedly in their papers about those who -- I guess something like 50 million, if I recall correctly; a large number of people -- who opt for the Do Not Broadcast.

MR. GUPTA: Yes. Thank you, Your Honor.

We're on the balance-of-hardships prong here. Really quick, big-picture point: There is no hardship from the existence of hiQ in real terms to LinkedIn or Microsoft. Their valuation quadrupled during the lifespan of hiQ. Microsoft today is trading at an all-time high. Putting hiQ out of business is not going to boost their market capitalization over the next period of time before we take this case to the next level.

Now, getting to the points that you asked about, the premise of hiQ's business is very simple. It's: "Public" means "public." They built a business around analytics on public information.

The most glaring silence in the papers of opposing counsel is on the fact that we cited a tremendous number of cases that say there is no expectation of privacy; that users

affirmatively publish on the Internet. And that could be published expressly with a public designation, which is what we're talking about in the context of LinkedIn.

We've shown you that there's a button. And I have a better printout if you want one today, but I can tell you what it says. It's, *Make my public profile visible to everyone*. "Everyone" is a strong word, Your Honor.

And when you hover over the information box for that, what it says is it will be visible to all LinkedIn members, as well as others who find you through search engines; e.g., Google, Bing, or other services. So it's everyone: The public, members, nonmembers, humans, and, to use their term, "bots." "Everyone" means everyone.

THE COURT: What's the record cite?

MR. GUPTA: That's Exhibit E to the TRO, Your Honor. I'll hand up a cleaner copy for you.

There you go, Mr. Verilli (indicating).

(Whereupon a document was tendered to the Court.)

MR. GUPTA: So, Your Honor, the case law that we cited actually shows that even when it's not designated public, and if it's just shared with a few people, you've lost your expectation of privacy under the law; but that's not what we're talking about here. We're talking about stuff that people affirmatively make public. Mr. Verilli is --

THE COURT: Well, what about those who also

affirmatively choose Do Not Broadcast?

MR. GUPTA: Okay. Let's talk about Do Not Broadcast. We were puzzling over what this is. What does it mean? We're talking about public profiles.

So the first thing I did is I asked my client, *What are they talking about? What is this Do No Broadcast argument that they're making?*

And my client's response was, *We don't do that*.

What they're accusing us of doing is something that Keeper doesn't do. Keeper doesn't provide this continuous feed of updates in to users' employers' HR departments.

What they've accused us of doing is: Every single change members make to their profiles goes to the employer.

The way Keeper actually works is a bunch of different factors are put into an algorithm, and out comes a composite score.

So it could say, you know, John Doe. He's at a -- he gets a score of 75. That's his score. That could include any number of factors. It's not actually the content of the changes. That would might be one factor, is: How frequently is he updating? But other things are huge contributors to that composite score.

Point is: What they're talking about is completely irrelevant to what Keeper actually does.

So I'm going, *What are they talking about here?* These are

some of the world's most accomplished lawyers. What are they talking about?

And I'm Googling it. And what I find is that there's actually a product they have, called "Update Me," which is something that's a part of their Recruiter product, which is a huge cash generator for them. And I'm handing up a true and correct copy of what I've printed out just yesterday.

(Whereupon a document was tendered to the Court.)

MR. GUPTA: So Recruiter has this Update Me feature. And the purpose of this feature is to know when to reach out to prospects.

I highlighted the first sentence here, because what they say is, *Every enhancement we make to our flagship product, LinkedIn Recruiter, is driven by our goal to make lives easier for recruiters like you*.

I thought that was sort of troubling, because we've heard so much in this case already about members first, members first, members first. Apparently, every decision they're making about this product has nothing do with members. It has to do with recruiters.

I highlighted the second bullet point, where they say what the product does. It alerts you when prospects make changes to their profiles, so that you can use those as signals to reach out at just the right moment. So they're providing this continuous feed of updates to their recruiters, who are paying

for a license.

And when you go to the next page, Your Honor, it gives you a little more detail on what this product does. And I've highlighted a sentence about three-quarters of the way down. So after you activated this feature on a profile by pressing the star button, what they tell you is from now on, when they update their profile or celebrate a work anniversary, you'll receive an update on your Home page. So any time a recruiter likes a candidate, they can turn on the Update Me feature. And then every time you visit your LinkedIn profile and make a change, they're going to have a notification. The recruiters are watching everything. When we talk about surveillance, that's surveillance.

When we're talking about what we do, we're talking about analytics on public information. We're taking the soapbox that the Supreme Court has talked about that the Internet provides, that -- everyone gets their own soapbox. They get to project their message to the whole world. We're taking that information, and making more interesting information out of it.

What they're doing is creating a system that allows them -- their recruiters -- to spy on people.

And the last sentence, Your Honor, is the real kicker. *And don't worry. They don't know you're following them.*

THE COURT: How do names get to LinkedIn Recruiter?

MR. GUPTA: Your Honor, the -- you mean how do they

find someone they want to --

THE COURT: Yeah. How does one even get on track?

MR. GUPTA: So, Your Honor, we have actually looked up the product collateral for Recruiter, because we've asked ourselves the same question. And it gets even more interesting.

So the Privacy Policy that they were talking about -- we quoted a few lines from the Privacy Policy in our reply brief on the Temporary Restraining Order. So here's a true and correct copy of the product data sheet for the Recruiter product.

(Whereupon a document was tendered to the Court.)

MR. GUPTA: And what it says here is pretty remarkable. So this is the candidate-search tool to find the perfect hire, even if they're not looking for a career move. *Zero in on the right person with 20-plus premium search filters*.

So they provide search filters. If I want, you know, a lawyer who knows copyright law, you know, I can -- I can find them using the search filters.

And the second bullet point is, *View full profiles for the entire LinkedIn network*. All 500 million plus members. Full profiles, Your Honor.

So what people are checking here when they're saying, *Give my profile only to my network*, or *Make it visible to no one* --

in this (indicating), that has absolutely no truth relative to recruiters. Recruiters have full access to the whole thing.

Now this gets better, because they've been talking about Privacy Policy. Right? Well, in our reply brief he cited a couple of lines from the Privacy Policy. And I'm just going to pull those up. So page 15 of our TRO reply brief. They've got -- we quote their privacy pledge. So the privacy pledge says, *We don't provide any of your nonpublic information, like your e-mail address, to third parties, without your consent*.

They're selling all -- they're selling all of your information to recruiters.

And then they say, *We do not rent or sell personal information that you have not posted on our services, except as described in this Privacy Policy*.

Hm. Really?

So, Your Honor, privacy here is a pretext, plain and simple. We're talking about public information. Let's not mix apples and oranges. This isn't about surveillance. We don't engage in surveillance. What we're talking about is allowing people to achieve their potential in their careers. LinkedIn has created what is a fundamentally lopsided situation. What they're doing is giving recruiters this incredible arsenal to look inside companies, and recruit them away.

All we're doing is saying, *Look. There's a lot of public information out there. There are advantages to employee*

retention. There are going to be stars within your organization you don't want to lose. We've got algorithms that will help you identify those stars, and give you a way to counteract this incredibly destructive process of -- of recruiting people out of companies.

Companies today -- if you talk with them, they're going to tell you that they have trouble keeping employees for more than five years. It's really, really hard to run a company. Can you imagine running a law firm or an organization, if it was such a revolving door?

So, Your Honor, Do Not Broadcast carries really no weight. And what we found in our research of was extremely disconcerting.

MR. VERILLI: So, Your Honor, might I --

THE COURT: It seems disconcerting to users all around. What you're saying is notwithstanding all of the privacy concerns, you're saying that -- sort of unclean hands; that LinkedIn has already doing all sorts of things that are at least as problematic as yours, so what's the big deal? Why not add one more straw to that camel's back?

MR. VERILLI: Your Honor, might I --

MR. GUPTA: Yeah. Your Honor, I do want to address -- Mr. Verilli did say a lot of stuff. So it's going to just take me a couple minutes.

My point is really much simpler than that, Your Honor.

I'm not making an unclean-hands argument.

What I'm saying is that "public" means "public." We're working on public information. We're doing stuff that has no privacy concern associated with it. And they haven't cited a single case that states anything to the contrary.

In fact, you'll see in our supplemental briefing we found that LinkedIn, itself, has made extensive argumentation of the same form in their own cases, where they've been accused of doing things like using people's contacts, and sending unsolicited e-mails to those contacts, inviting them to LinkedIn. And their rationale in those cases was, *Well, everyone knows your a member of LinkedIn, because you have a public profile on LinkedIn, so there's no additional privacy violation. That was your own affirmative act of making it public*.

So what I'm saying is this is really uncontrovertible territory that we're talking about here. We're talking about stuff that actually both companies agree on.

I want to talk a bit about the User Agreement. So the User Agreement doesn't contain any -- any clear waiver. The User Agreement is a -- is a hornets' nest of contradictory information. It says -- if you walk through the Don'ts in this Agreement --

THE COURT: Which tab is this, again?

MR. GUPTA: So this is Exhibit B to the

Rockwell Declaration.

THE COURT: Yep.

MR. GUPTA: Okay. So if you go to the Don'ts, which is a section near the end of the document --

THE COURT: Section 8?

MR. GUPTA: I'm sorry. Did you find --

THE COURT: Section 8?

MR. GUPTA: Yes, it's in Section 8.

There's a whole series of don'ts here, and these include -- when you go through them and read them carefully, they include things like -- so, for example, the fourth from the top. It says, *You can't scrape or copy profiles and information of others through any means, including crawlers, browser plug-ins and add-ons, and any other technology or manual work*.

So you can't copy a profile through manual work. Yet, in order to use the profiles, you have to access these things, and you have to make a copy to -- at least to your computer.

Furthermore, there's actually a feature on the profile that allows you to save a copy to your own computer, thereby creating a manual copy. And then you can print it. There's -- it says you can't share information of others without their express consent, yet their user interface actually has a Share button on it. It even says you can't manually access the site, which is extremely ironic in this context. Everybody's,

apparently, in violation of their terms of agreement -- of their User Agreement, just by using the site.

THE COURT: Which number are you looking at?

MR. GUPTA: So that one is --

THE COURT: Is it 8.2? Don't?

MR. GUPTA: It's -- it's in the Don'ts. So if you go to the fifth from the bottom, it says, *You can't use manual or automated software -- manual or automated software, devices, scripts, robots, other means or processes to access, scrape, crawl, or spider the services or any related data or information*.

So these are just extremely overbroad. And there's no way you could not allow your users to manually access the site.

But anyway, Your Honor, the point is this User Agreement, if -- if --

First of all, those Don'ts don't even survive termination. So they terminated hiQ from the Agreement. And if you look at what expressly survives termination, these Don'ts do not survive termination. So you're absolutely right.

The other thing to keep in mind is that this Agreement has a dispute-resolution provision in it: Section 6. And Section 6 says, *You agree that the laws of the State of California, excluding its conflict-of-law rules, shall exclusively govern any dispute relating to this Agreement and/or the services*.

So if they're going to introduce the User Agreement into this dispute, then this dispute relates to the User Agreement.

And they've got no CFAA claim anymore, because that's federal law.

And all their preëmption arguments are out the door.

So this is just -- this is all theatrics. It carries absolutely no legitimate weight.

Your Honor, the *Don't scrape or don't automatically collect information* statements that are in here -- all of these self-contradictory statements in the User Agreement are clearly contradicted by what the users actually read and actually click on, which says, *Make it public to everyone: Visitors, members, humans, and bots*. That's what people are asking for. That's what they're consenting to.

MR. VERILLI: Your Honor, may I respond?

THE COURT: Yes.

MR. GUPTA: Your Honor, I did want to just --

THE COURT: Well, I want to move on.

Go ahead briefly, please.

MR. VERRILLI: Yes. Several points.

Let me start where Mr. Gupta finished. If Your Honor looks at the document he handed up, the very top of it, what it says is that by -- what you're agreeing to is making the information visible. Visible. That's what you're agreeing to here, and that's it.

Second, with respect to his points about Do Not Broadcast, I think, with all due respect, Your Honor, he did not answer Your Honor's question. He says he points to their algorithms.

Well, of course, their algorithms focus on whether LinkedIn members change their profiles. That's what drives up their score.

THE COURT: Well, when you say "focus on," how do I know how big a factor it is?

MR. VERILLI: Why -- well, why don't you ask Mr. Gupta whether a change in the profile makes a difference, and how big a factor it is.

But then in addition, Your Honor, with respect to this Recruiter point, now, this wasn't made in the briefs. And I apologize to Your Honor that I'm not fully able to respond to it, but with all due respect, it's a bit of an ambush here. And we will find out. We will find out what information is -- relevant information with respect to this Recruiter product; but one thing is clear on the face of it is that that's not information that goes to your employer. So that's not information that compromises your privacy and your employment status in the way that their product does.

And if I could just ask Mr. Blavin to make a couple of additional points.

MR. BLAVIN: Thank you, Your Honor.

And our client is here, who just confirmed that LinkedIn's understanding is that when the member selects Do Not Broadcast, that the Recruiter product respects that, and those changes are not notified to the recruiters.

Moreover, the Recruiter product is entirely different than hiQ's product. The Recruiter product is where the recruiters are reaching out to people about job opportunities. People would welcome that. There are new opportunities out there.

Their product is doing something entirely different.

THE COURT: What information -- what warning's given? Because you placed such a premium on protecting the privacy rights of your users, where are users informed that no matter what setting they pick, public or not, it appears that recruiters will have access to that?

MR. BLAVIN: Well, with respect to recruiters, if you look on the Privacy Policy, Section 2.12, Talent Recruiting, Marketing, and Sales Solutions -- I believe that's Exhibit C to the Rockwell Declaration -- it explicitly states that user data is made available to recruiters.

It goes on to say that you may limit --

THE COURT: Where are you looking at? What section?

MR. BLAVIN: 2.12. I just want to make sure that's the right exhibit.

THE COURT: It says, *You may limit or prevent such subscribers from exporting your profile information by*

configuring your public profile visibility settings --

MR. BLAVIN: Correct.

THE COURT: -- *restrict access*.

MR. BLAVIN: And moreover, if you select Do Not Broadcast, that means those changes -- those notifications -- are not made to the recruiters on a continuous basis.

THE COURT: Well, how does that square, though, with this alleged collateral here that says that you can view full profiles of the entire LinkedIn network, not just those who select public view? Because all 500-plus million --

MR. BLAVIN: Well, that's -- that's a collateral material that's made to advertisers.

These are the privacy profile settings which are described to the users.

THE COURT: Well, when you "just" -- this is coming from -- if this is an authentic LinkedIn.com website. So representation is made. You're saying this is not a truthful representation?

MR. BLAVIN: No, no, no. All I'm saying is that, as a general matter, yes, all profile information for members is visible --

THE COURT: Well, then how can that be --

MR. BLAVIN: -- subject to the privacy policies.

THE COURT: How is that consistent with 2.12?

Because it just said you can configure your profile-visibility settings to restrict those fields.

MR. BLAVIN: I think it's a general collateral material describing that member information is available, obviously, subject to the privacy-policy protections which LinkedIn is committed to its users to do, which is made explicitly clear in 2.12. And Your Honor, again, we've just been thrown this --

THE COURT: Well, at some point let's step back.

You are placing a lot of your arguments about business model, protecting the privacy, maintaining the trust and integrity of your user base, based on, frankly, fine print of various policies which, assuredly, a very small percentage of the people of your users would actually read and understand. What they're likely to look at is when they actually make the choice that's on the Web page. That doesn't have all of these qualifiers.

So, you know, we can sit here for nine hours, and you go through every damn piece of paper. And, frankly, I don't find that convincing.

MR. BLAVIN: Your Honor, if I could quickly respond to that.

THE COURT: You're the one talking about business model, and putting the privacy rights of your users so high; but frankly, you're doing that on a legal basis that I don't

find, in the real, practical world, very persuasive --

MR. BLAVIN: Your Honor --

THE COURT: -- so let's move on to something else.

MR. BLAVIN: Just very quickly, to respond to: Is it in real time? When users make changes to their profile, this is in the supplemental Rockwell Declaration. Right there, with respect to every change, they have the option of not broadcasting it. That is not buried in a Privacy Policy. That is made clear to the user.

THE COURT: That's your best case.

So what's your response to --

MR. GUPTA: My response to that --

THE COURT: -- how much effect --

I don't know what your algorithm is -- maybe you don't know exactly -- but how do I know there's not a fairly close one-to-one correlation between number of changes, and ranking? That number of 57, or whatever it is.

MR. GUPTA: Your Honor, what I'm told is that there are a lot of factors. I don't know how many factors. I don't know what the weighting is.

But I can tell you one thing about this Do Not Broadcast argument, just to finish it off. This idea that there's this moment of consent when the user clicks the radio button that says Do Not Broadcast -- the problem is the law recognizes consent if it's informed consent.

And the document that we handed up to you explained that the Recruiter product, when it's doing this Update Me feature -- what we're calling, to use Mr. Verrilli's term, "surveillance" -- that it says, *Don't worry. They* -- the user -- *don't know you're following them.* The user doesn't know that the recruiters are following them.

THE COURT: We're not on the same -- yeah. You already said that; but what does that have to do with my point?

You're saying they violate expectations, so you can go ahead and violate?

MR. GUPTA: No, that's not what I'm saying, Your Honor.

THE COURT: It sounds like it. I'm asking you a question.

MR. GUPTA: Right.

THE COURT: And in most -- unbeknownst to most users, this thing exists. In fact, you apparently just found this yesterday. Otherwise, you would have included this, I hope, in your supplemental --

MR. GUPTA: Oh, absolutely, Your Honor.

THE COURT: -- rather than springing it on counsel and the Court the last minute.

MR. GUPTA: Yeah.

THE COURT: So the chances of an actual user knowing of this now acting responsively and informing their decisions

are very, very small, when you, lead counsel, didn't even find this when it's the center of your case.

So the question still -- and I guess you've told me now you can't answer this. To the extent people have opted for -- and I'm going to forget all of this collateral stuff; all of these fine prints; Exhibit Triple E to some declaration. The thing that people see says, *Don't Broadcast*.

And if that, in fact, results in -- if changes do have a large influence on whether they become ranked highly on Keeper, that makes it more problematic. I'm not saying that's dispositive. That creates a potential problem; but apparently you can't tell me how much influence. There's this black-box algorithm, and so we don't know, as we sit here.

MR. GUPTA: Your Honor, there's -- I don't know. And the employer doesn't know, either. So it kind of -- it's not a signal that someone is updating their profile in any meaningful way, because no one actually knows the trade-secret algorithm. That's the best I can tell you right now. Your Honor, if you'd like me to follow up, I'm happy to.

THE COURT: Well --

MR. WISOFF: I'd like to make one other point on that --

THE COURT: Make it short. We've got to move on.

MR. WISOFF: -- Your Honor, and that's that this notion that the broadcast feature is a statement by the user

that they don't want anyone to know that they've made changes to their profile is a pretty big leap of faith.

What it says is that every single time you make a change, it's not --

All of your contacts -- the people that you are connected with within LinkedIn; other LinkedIn members -- are not going to get an e-mail telling them that you've made that change.

THE COURT: So you're saying there are other reasons why --

MR. WISOFF: Well, certainly --

THE COURT: -- one would not turn that setting off.

MR. WISOFF: Absolutely.

From my perspective, I don't like it when I get bombarded with e-mails from all of my contacts about every little thing they've done. In fact, on a Facebook account I sometimes get an e-mail telling me when somebody's having dinner at a particular restaurant in Philadelphia. That's not really very important to me. And, in fact, it's somewhat annoying to me.

So to say that because people have checked this box, that they somehow want to override the public-visibility setting that they actually affirmatively agreed to, when all they're saying is they don't want every change sent by e-mail to their contacts, is a pretty big leap of faith.

The other point I would make is we keep talking about the consumers' expectation of privacy. And I would submit, Your

Honor, we're not writing on a clean slate here. There have been vast numbers of legal decisions that say as a matter of law there is no expectation of privacy in information posted on a public website.

And, in fact, there are quite a few cases -- and these were cited in our supplemental brief, and also in our original papers -- that say that even where you have selected your settings to be private, and not to share with the whole world, you still don't have an expectation of privacy, because once you've shared with some people, there's no expectation that those people won't share it with someone else.

So I think when we are talking about an expectation of privacy, we're in an area that's not just embodied in contract; it's embodied in well-established doctrinal law that says when you make your profile public, you have made a choice. There are pros. There are cons.

And every time you go out on the World Wide Web, there are all kinds of programs that are using your personal information for all kinds of purposes that you don't know about. And maybe at some point in time, Congress will pass a law that regulates that and puts restrictions on that; but right now what LinkedIn is trying to do is to restrict anyone that has any potentially competitive business from using what has become the world's largest database -- one of the most valuable databases in the entire world that has 500 million people in it -- on a scale

that is unimaginable.

And to say that they can raise these privacy issues, when they are reserved -- not only reserved to themselves, but are actually going out and selling the same information to other people for their own purposes, is the absolute hypocrisy. It is an absolute pretext.

THE COURT: Let's get on to the merits. Preview the merits question. And the front question is the CFAA, because if the CFAA applies, number one, that preëmpts all your state law causes of action.

MR. GUPTA: We disagree with that, Your Honor. And we hope to have some time to talk with you about that. We completely disagree with that.

And the perhaps the most emblematic case that refutes that point is *Nosal I*, where Judge Kozinski wrote very clearly that the CFAA was enacted interstitially, and that it does not displace common law, and that does not --

THE COURT: It doesn't displace. It's not field preëmption; that is, if something that violates is found not to violate the CFAA, does that mean that that doesn't violate some state law.

But if something does violate, if conduct is deemed illegal under federal law, a state law can't make it legal. That's obstruction preëmption.

MR. GUPTA: Your Honor, that's a direct-conflict

argument that they have made --

THE COURT: Yes.

MR. GUPTA: -- but we disagree with that, because nothing in the CFAA talks about revoking authorization, and nothing requires them to revoke authorization.

So it is often the case that people will make a choice to exercise some statutory right; but the choice to exercise a statutory right needs to be scrutinized under law that's intrinsic to that statute, itself. It happens all of the time, Your Honor.

So, for example, take another federal property right, patent law, governed in many cases by equitable estoppel doctrine. There are cases like *Qualcomm versus Broadcom*, which have said that even though you own a validly issued federal property right, you can't exercise it in a way that's inequitable.

And that's exactly what we're saying here, Your Honor, is that the statute doesn't talk about revocation. It doesn't set forth conditions for revocation. It doesn't purport to require revocation. And it certainly doesn't talk about revocation of access to public material. That was never within the contemplation of the statute; but the point is that there's plenty of law that says you cannot exercise these rights as weapons against other people to carry out unfair competitive aims.

Another example of that is *U.S. versus Microsoft*, another federal property right, which is the copyright right, where the D.C. Circuit, when approving the consent judgment against Microsoft, said that Microsoft made an argument that, *Well, we owned duly issued copyrights on all of our Windows software, so we can go out there and put all of these onerous restrictions on our licensees*.

And the D.C. Circuit said that that borders on frivolous. And it said that that's like saying, *Because I own a baseball bat, I can do whatever I want with it*.

THE COURT: Well, but has to be frivolous in order for it to be unenforceable; doesn't it?

MR. GUPTA: I don't think so, Your Honor. I think that -- I don't think that was a legal requirement.

I think the Judge was a little bit -- bristled at it.

The citation for that, Your Honor, is 253 F. 3d. 34 for the *U.S. versus Microsoft* case.

And the *Qualcomm versus Broadcom* case is 548 F. 3d. 1004 Federal Circuit 2008, where equitable estoppel prohibited the exercise of patent rights against a particular standard -- products that adhere to a particular standard, because Broadcom had not disclosed its patents to the standards-setting organization.

THE COURT: Isn't that a matter ultimately of federal law incorporating common-law principles? You're saying that's

a stand-alone state law that --

MR. GUPTA: Your Honor, the equitable estoppel doctrine could be arguably a federal common law doctrine, so I don't know if it would qualify as a state or federal common law; but my point is simply that a federal property right, to the extent it may exist, does not exist bereft of a matrix of regulations on how you can use those property rights.

THE COURT: Well, that still ultimately is a question of federal law, and whether it recognizes a defense that incorporates certain matters; but to say, for instance, that the California constitutional right of free speech could preëmpt -- reverse preëmpt, I guess -- a federal statutory -- or prevent somebody from exercising statutory rights -- that seems odd to me. I mean --

MR. GUPTA: Your Honor, it --

THE COURT: Assuming it's not a *Noerr-Pennington* problem.

MR. GUPTA: Yeah. Your Honor, so on this point, to me, it strikes me as a very straightforward point, because if you think about -- they used a metaphor of trespass. They're -- a lot of their argument is based on the CFAA as a trespass statute.

Well, the case of *Marsh versus Alabama* and the case of *PruneYard* -- these are all cases that talk about fundamentally trespass. And what they say is that the physical trespass law

needs to cede to free speech principles.

And so these property rights always exist within a matrix of other rights.

THE COURT: Well, that's a property right that accedes to a federal constitutional right. There's not a Supremacy Clause problem there. That's a question of whether or not, you know, in the hierarchy of things, a constitutional right prevails. I'm talking about state and federal. Let me ask --

MR. GUPTA: Your Honor, Your Honor, I just have one example. I want to just --

THE COURT: One more example, and then I want to --

MR. GUPTA: Let me give you an example, which is if the CFAA had this sweeping, unbridled power of revoking authorization to anyone, it would lead to incredibly absurd results.

So let me give you an example. Let's say that I'm a Web hosting company. And you're hosting your business' services on my servers. So we have a contract governed by California state law. In that situation, I owe it to you that I'm going to continuously provide service to you for three years.

Under their interpretation of the CFAA, I could simply revoke your access to the server. You can never come onto the server again, which you have a contract with me for. But the CFAA action that I took would preëmpt California law. And, to

boot, you know, there's all of these other consequences of the CFAA that are unspeakable.

THE COURT: So your argument is, for instance, whether or not there's a valid withdrawal of authorization which would be necessary in order to trigger CFAA protection might be governed by state law? State contract law?

MR. GUPTA: Yeah. The conditions and motivations and circumstances under which somebody might choose to revoke access under the CFAA would need to be governed by overarching principles of equity, common law, unfair competition. It's not a weapon.

THE COURT: All right. What's your response on just the preëmption question?

MR. VERILLI: Yeah. So Your Honor's quite right that if the CFAA applies. It preëmpts all of their causes of action.

I would just note -- and I want to go into preëmption in depth, but I would just note for Your Honor's focus here that before you get to the question of preëmption, they have got to have a likelihood of success on an affirmative cause of action that justifies the injunction that they've claimed, preceded by the intentional interference or unfair competition.

THE COURT: Well, the preëmption would make that difficult, because you don't even get to those if there's preëmption.

MR. VERILLI: Right, right.

THE COURT: That's why I took that first.

MR. VERILLI: Yes, yes.

THE COURT: If there is no preëmption --

MR. VERILLI: You're totally right about that, Your Honor --

THE COURT: -- then you have to get to their merits --

(Reporter requests clarification.)

MR. VERILLI: Forgive me.

You're totally right about that, Your Honor, but the reverse is also true, in that if they don't have a viable cause of action, you don't need to get to the preëmption. And that's what I'm saying. You can resolve it either way. Under either one --

THE COURT: I understand.

MR. VERILLI: Now with respect to preëmption, I think the right thing to do here is to focus on the relevant statutory materials and the relevant precedent which address the scope of the CFAA, and which indisputably lead to the conclusion that their claims are preëmpted.

And I don't think there's any serious dispute here that we're within the plain meaning of the terms of the CFAA. This is unauthorized access resulting in obtaining information that inflicts more than $5,000 worth of damage, so we're within the

plain terms. We have an express private right of action entitling us to relief under those terms. We're within the plain terms. And there's no doubt about that.

They're making an argument that the plain terms need to be read more narrowly than they -- than they, on their face, clearly state; but I would submit, Your Honor, that binding Ninth Circuit precedent has already definitively rejected the very argument they're making about the need to narrow the scope.

THE COURT: Well, I want to talk about the CFAA in a moment, but before we get there I just want to hear the predicate about what the consequences of finding a CFAA application here. And is there an exception to preëmption?

One of the arguments Mr. Gupta's making is that, yes, even if the CFAA were generally applicable, if it is misused in a way that violates certain state rights like breach of contract or perhaps breach of the law of unfair competition to monopolize -- the use of monopoly power -- that there is room for state-law limits on the employment of that CFAA cause of action.

MR. VERILLI: Yes. I don't think there's -- there's absolutely no authority for that proposition. Your Honor has zeroed in on exactly the right points with respect to the *Microsoft* case and the *Qualcomm* case. In those cases, those were both instances of reconciling two different strands of

federal authority, and making them work together.

They have not cited a single case -- and I'm not aware of a single case -- suggesting that a federal statute's squarely on point, and applies, and creates a particular right or creates a particular prohibition that -- based on some kind of equitable notion, that that would be unfair under state law; that the federal statute doesn't apply. There's no case for that proposition. It's a direct refutation of the Supremacy Clause.

Now, the -- this is, as Your Honor correctly identified, a question of conflict preëmption here, but in -- but I think it's worth remembering that what my friends on the other side are doing here is asserting an affirmative right to get injunctive relief that would require us to disable our technical measures so they can get on our website and get on our servers, in contravention of our policies.

And so what we've asserted is our right under the CFAA to block that unauthorized access. And, having asserted that right -- and we believe that we're clearly in the right here. And I do want to talk about them finding Ninth Circuit precedent on the question of the scope of the CFAA.

But having asserted that right, if we are correct that we have a right --

And, as I think we've pointed out in our brief, *Power Ventures* specifically describes the CFAA as a computer trespass

statute. Its function is to provide remedies against unauthorized access that are in the nature of a trespass.

And if that is what they are doing, they are violating the -- they are violating the very thing that federal law exists to protect. And --

THE COURT: Well, let me ask. You place emphasis on sort of the trespass notion. The Ninth Circuit has referred to the CFAA as kind of a digital trespass statute. What's your opinion of Professor Orin Kerr's analysis, if you read that?

MR. VERILLI: Yes, I have. I think --

THE COURT: And, you know, looking at trespass now through the lens of norms and silent expectations --

And the starting point, as he posits, is that the World Wide Web is presumptively open. And once you've placed something on the Web, it's like putting it on the town square. There are ways of taking it out of that arena, and thereby invoking protection in the application of that CFAA. That de-emphasizes use of authentication techniques and what you calls "bumps in the road," you know, like, you know, certain IP disablers and other things that may make it difficult.

But his view is that there should be a presumption under -- borrowing from the normal methodology of trespass evolution law applied in the digital domain to start with a very powerful premise that anything on the Web should be presumptively open, and not subject to criminalization, even if

you get around these -- what he calls "speed bumps" on the CFAA.

I take it you may not agree with his sense of it.

MR. VERRILLI: Professor Kerr is a smart law professor. He's wrong about this.

Judge Breyer, in *3Taps*, is right.

But I think even more importantly, the Ninth Circuit has already definitively rejected that very argument. And you can see it in two cases. The first is in *Power Ventures*.

And if the Court looks at page 1067 of 844 F. 3d. in *Power Ventures*, the Ninth Circuit sets out the standard for when the CFAA applies. And it says that -- acknowledges that a violation of terms of use of a website, without more, can't establish liability under the CFAA, but it does say -- and this goes to a point Mr. Gupta was making earlier, and definitively refutes that point. It does say that, *and then you can run afoul of the CFAA when a person has no permission to access a computer, or when permission has been revoked explicitly*. So it's right there. The Ninth Circuit definitively interpreted the CFAA to cover revocation. *Once permission has been revoked, technological gamesmanship or the enlisting of a third party in gaining access will not excuse liability*.

THE COURT: But neither Facebook -- Facebook does not address the situation. There, I mean, arguably, the defendant was able to kind of get into the website and obtain data on

usage and facilities in order to -- I forget whether it was broadcast e-mails, or send out communications. That was not just using publicly available data. I mean, so the Court didn't have to address this question that Professor Kerr --

MR. VERILLI: So I want to get back --

THE COURT: It was more traditional trespass. It was getting into the system; deep into the system.

MR. VERILLI: I want to get back to *Power Ventures*, but I do think *Nosal II* -- and that's, of course, a case Your Honor's very familiar with. But in *Nosal II* -- and I think this is at pages, if I'm remembering correctly, 1037, 1038 of *Nosal II*. There was a question about whether the Jury Instruction in that case was correct as a matter of law. And the argument was that you couldn't have, under the CFAA -- the defendant's argument was, *You can't have a violation of the CFAA unless, at a minimum, there is a technological barrier in place that impedes access*.

And what the Ninth Circuit held in that case was that there is no such requirement under the CFAA; that it's not within -- the plain terms of the statute don't impose that requirement, and it would make no sense to impose that requirement. That's what the Ninth Circuit held in the case.

And, of course, they're asking you to go a step beyond *Nosal II*, because in *Nosal II* the argument was, *So you have to show evasion or overcoming of technical barriers*.

Well, here we have the evasion or overcoming of technical barriers.

What they want to do is go further and say, *You can only violate the CFAA when you've got a wall up, with password protection*. I just think it's definitively refuted there.

And now if I might go back to *Power Ventures*, because I want to direct Your Honor's attention, if I could, to the next page after the one I was quoting, because I think this also, even taking Your Honor's point, definitively refutes the position of my friends on the other side. So what the Court said and held in *Power Ventures* was that for Power to continue its campaign against -- campaign using Facebook's computers, it needed authorization both from individual Facebook users who control their data and personal pages, and from Facebook, which stores the data on its physical servers. Permission from the users, alone, was not sufficient to constitute authorization after Facebook issued the cease-and-desist letter.

Now, what the Court is saying there -- and I would submit it's saying in very plain terms -- is that the argument that my friend on the other side is making that once users make this information of theirs public or available to be visible, at least, on the Internet, that at that point, that the entity that controls the computer or server on which that information resides loses all authority -- loses all authority to control the use of bots to scrape that data, or other unauthorized

incursions.

Well, *Power Ventures* expressly rejected that exact argument, saying *It's not enough that it's okay*. Because remember in *Power Ventures* it was okay with the users. They had agreed to let Power have access to their data. And the Courts --

So that's a step beyond here, where, of course, because of the issues we were talking about earlier this afternoon, they don't have that kind of affirmative agreement.

THE COURT: Well, but I think the focus that you're focusing on, as well as *Nosal* -- the main focus on *Nosal*, as evident by the dissent from Judge Reinhardt, was: Who has the power to grant that consent?

And the Ninth Circuit has come down squarely that it has to be consent of the operator of the site. If there is no -- if there is no authorization in that sense, there is no authorization.

But the Professor Kerr point is a much broader -- it's a different issue. It's not a question of whom. It's a question of what. Is there, quote, "unauthorized" access being obtained to data that is otherwise open to the public in a way that's different from breaking into Korn Ferry's database, or getting into Facebook's?

And neither of those situations deal with this, I think, emerging issue, where there hasn't been a lot. And I think

Judge Breyer's decision is the one that comes closest to otherwise publicly available data to which certain speed bumps have been placed; technological speed bumps.

Is that the kind of thing that can be deemed subject to criminalization, within the meaning of the CFAA?

MR. VERILLI: I guess what I would say, Your Honor, in response to that: It's within the plain terms of the statute. There's simply nothing in the statute that supports drawing that line.

The Ninth Circuit has not drawn that line, and could have. It drew a line differently to try to deal with the problem that I think professor Kerr is trying to deal with. And that's why the Ninth Circuit requires the cease-and-desist letter. It says that the terms of service, alone, aren't enough, because it may not be clear enough that you're engaging in an unauthorized intrusion; but once you get a cease-and-desist letter -- and particularly when you get a cease-and-desist letter, and that's in combination with the owner of the computer or the owner of the server using technical measures to try to block your access -- when those conditions are present, then you're in a situation in which there is nothing unfair or untoward or improper about enforcing the CFAA, and granting the owner of the computer, the owner of the server, the right to enforce the terms on which this information will be made available.

THE COURT: Well, that's certainly true from the perspective of procedural due process and notice, because there, there's no question you've got notice, and so any deauthorization is well known. It's not a question of, you know, being surprised.

I don't know if it answers the larger question.

But I do want to ask you. I mean, I think the most powerful argument is that the plain language of the statute talks about accessing a computer without authorization.

MR. GUPTA: The simplest response to that, Your Honor, is the plain language of the statute says nothing about revoking authorization. It does not mention the concept of revoking authorization. The predicate of not having authorization under the CFAA is simply not having the rights, as a matter of user name/password-type credentials, to get into the system. And so when an employer revokes your authorization, your user name and password no longer work, and so you are without authorization.

That is the situation that has come up for the Ninth Circuit. This is a --

The idea that they can drive this truck into words that aren't in the statute -- that "revocation of authorization," because in these cases the Court focused and used those words -- doesn't create enough capacity for the idea that all public information could have been --

THE COURT: I guess I don't understand your argument. You're saying that because the CFAA doesn't contain the words "revoke," that "without authorization" can only mean without authorization from the get-go, and not change?

MR. GUPTA: Your Honor, the point is that the entire framework of the CFAA was not contemplating a situation where people were plugging servers into an open Internet, and by virtue of simply putting the server onto the Internet, people could grab information from it.

That's the beauty of the internet. It's a big, public, open Internet. There is no initial authorization. It's just a physical act.

And when the CFAA was being enacted, they were thinking of authorization in the conventional, mainframe type of thing, which is, *I have an employee. I need to authorize the employee*.

THE COURT: No. I understand that. And, in fact, the CFAA started off with, as I recall, criminalization of hacking into government computers, and it was expanded two years later to include private computers, all well before the worldwide Internet became the World Wide Web. And so, you know, it's not hard to ascertain that Congress didn't have this in mind at the time. But what does one do?

I mean, I understand all of the policy concerns and the implications. And if suddenly you criminalize anybody who, you

know, wants to have access to a business competitor, a political rival, or anything else, and wants to do research, and some government agency doesn't want them doing research, and all the implications, in terms of the marketplace of ideas -- but what do I do with this plain, seemingly simple language?

"Accessing." Is there something secret about, nuanced about the term "accessing a computer" -- we know what that is -- "without authorization"?

Well, if you say, *Well, "without authorization" only means without initialing authorization, or you can't deauthorize when it involves the World Wide Web* --

MR. GUPTA: No, Your Honor. I think that it's -- I think -- you know. Look. Judge Kozinski already found once that that phrase, including the "exceeds authorized access," is ambiguous. We're not asking you to go out on a limb here.

Authorization is ambiguous, because even -- even Mr. Verrilli and I can disagree about whether these IP blocks constitute a deauthorization. Right?

I will point you to *Facebook versus Power Ventures*, where, in Note 5 what they say is the opposite of what Mr. Verilli is saying. They say simply bypassing an IP address would not constitute unauthorized use.

We're talking about speed bumps. Right? And Professor Kerr talks about speed bumps. Do speed bumps count

as authorization or deauthorization?

Our position is: Absolutely not.

Their position is: Absolutely yes.

So the language is undeniably ambiguous in the context of the modern Internet. And all we're saying is let's not fool ourselves, and say that this language is unambiguous. There is no authorization that happens, beyond just plugging in that computer, when somebody sets up public pages.

Your Honor, I did -- I actually want to cede the floor, because obviously a huge part of this argument is the principle of constitutional avoidance, but I just wanted to make two quick points. The first is that Mr. Verilli sort of presented this sky-is-falling scenario of, you know, if the CFAA doesn't allow them to kick us off, then they lose all authority to control what's happening on their computers. And obviously, that's not true. There are plenty of other bodies of law that give them the ability to regulate malicious hacking and other types of damaging activity.

THE COURT: Well, what would you do if you're hit with 95 million attempts a day, many of which may well be some attempt at hacking? You don't know for sure. You have to really just --

MR. GUPTA: Your Honor, so I think that --

THE COURT: What are you supposed to do in that situation?

MR. GUPTA: So this is a point that Mr. Verilli made earlier, and I didn't have an opportunity to get to, which is they get these 95 million attempts each day from people, and they're trying to block these visits. So these are people who are trying to protect their user-privacy issues. They rationalized it in the Rockwell Declaration on three grounds as to why they're blocking this information.

They said there's user-privacy issues.

And they said that it's to prevent identity theft and other fraud.

And they said it's to ward off denial-of-services attacks.

So protecting user privacy and preventing identity theft have absolutely no relevance to public pages. Case after case has held that public pages don't present a privacy concern.

The third is this warding off of denial-of-services attacks. We don't disagree that they have the right and they have the necessity to fight off these malicious intruders. And there are entire companies, entire businesses, security industries, built around that.

This is not what we are talking about here today. What we are talking about is they are trying to block a low-volume user who is not engaged in a denial-of service attack from accessing public --

THE COURT: But your injunction would --

I mean, are you acceding or do you acknowledge that they

would generally have the right to use bot blockers?

MR. GUPTA: Your Honor, they would have to use -- any kind of blocking mechanism would have to be narrowly tailored, and at a reasonable time, place, manner restriction from a free-speech point of view, and it can't be anticompetitive.

What they're doing here is obviously competitive.

THE COURT: So they would have to identify the source of each bot attack to determine whether that's a legitimate -- whether that's a competitor, a potential competitor, versus a hacker, versus a foreign agent attempt at surveillance, or something else? I mean --

MR. GUPTA: Your Honor, my understanding is, if you look at their papers, they've listed four or five different types of protections that they use on their system. Most of them are designed to prevent large-scale intrusions that would -- that would impair their servers.

All we're saying is they cannot block us. They cannot block hiQ, which is trying to access public pages. They can't block for motivations --

THE COURT: So if they knew, for instance, that a particular user --

Let's say if you accede that they could have a general policy and have a general defense, a technical defense, I take it your position is that once they are aware through exchange that you are a user that doesn't fit into one of those threats,

that they would then have to "open the door," so to speak?

MR. WISOFF: I don't even think you have to go that far, Your Honor. We're asking for preservation of the status quo. So to the extent they had general blocking mechanisms in place, you know, we're not asking, as part of a preliminary injunction, at least, for removal of that.

What we're saying is that they --

And you raised this issue. Mr. Verilli raised this issue that we have to win on our affirmative state claims, or show that we have a likelihood of success on those in order to win here. I actually don't think that's entirely true.

And as we said in our supplemental brief, as a practical matter, it is only the CFAA Penal Code threat that they have made that -- and the criminal liability that attaches to that, that, as a practical matter, keeps us from coming back to the site, because --

THE COURT: So would you be satisfied with an injunction that's essentially a declaratory relief injunction?

MR. WISOFF: An injunction that they can't give force and effect to the CFAA Penal Code revocation, until the merits of whether those statutes apply, and how they apply, have been decided, because we've been able to gather data under the status quo with these mechanisms in place. Because these pages are publicly accessible, we've been able to do that prior to the lawsuit.

We just want to be able --

We don't want to be put out of business before the merits can be determined.

And so we're not asking the Court to say they have to take down all technical measures that generally block unidentified automated bots coming onto their site; but to the extent that they've specifically blocked our IP address, and have specifically -- are trying to criminalize our access to the website -- I mean, under the CFAA, even individuals can be criminally liable if they cause their company to access the site. So --

THE COURT: All right. Let me go back to the first question, then. What is your argument in terms of -- in the face of fairly -- what appears to be, at first glance, plain language?

I guess you're arguing that "authorization" is not plain; it's ambiguous.

Although if you read *Nosal II*, the Court goes to great lengths to talk about how that's plain language. It goes through just about every Circuit in the nation to back them up on that. So I'm not sure.

MR. WISOFF: Your Honor --

THE COURT: Maybe your argument is that in this context, in the context of the World Wide Web and the Internet, that "authorization" or "without authorization" has a different

meaning, not addressed by the Ninth Circuit or any other Circuit at this point.

MR. WISOFF: Correct.

MR. GUPTA: Right, Your Honor.

MR. WISOFF: That's our argument, because these cases that you're talking about --

You know, Mr. Verilli made a point that you don't have to, you know, have -- to contradict Professor Kerr's opinion, he talked about how it's not necessary to have a technical barrier like a password.

So you know, obviously, I can't walk back into your office, into your chambers, and look at your computer. I don't have authorization to do that. That information was never meant to be public.

So whether you have a password on your computer or not, that still falls within the CFAA, because the purpose of this statute was to protect information that's not generally available to the public, that only certain people are authorized to access.

But when you put up a website and you program a server to respond to every request, by definition, there's been authorization for the entire world.

And the idea that you could send a letter to one of billions of people who visit that website every day and say, *If you ever type our URL address into your computer while you're*

sitting in the privacy of your home to view information that is public for every other person in the world to see; that that's a criminal -- a federal criminal violation, I submit, Your Honor, that you have to duty not to interpret a statute to lead to such an absurd result.

THE COURT: So you would say that once you place it on a public setting for the World Wide Web, that is authorization? Even if you later attempt to delimit or revoke that individually on a case-by-case basis for purposes of the CFAA, that is not unauthorized?

MR. WISOFF: I can't imagine that Congress intended to criminalize that activity, or that any interpretation of the statute that would lead to that result would be a sensible interpretation, number one.

Number two, to the extent you are going to analogize to trespass law, trespass law has always lived in conjunction with other laws of general application. And we're not talking about a private home. And we're not even talking about a mom-and-pop business, but in the context of a mom-and-pop business, one of the cases they cite, *Alexis versus McDonald's Restaurants of Massachusetts* -- there is a Massachusetts trespass statute where somebody came into a restaurant, and the question is; whether they were properly thrown out or not. And the Court said that the statute on its face didn't admit of any exceptions of an owner's ability to exclude, but that the

statute has to be read within the body of other laws. And so it said, absent some invidious, ulterior purpose, then once proper notice has been given by the owner, the business licensee remains. He's subject to arrest.

So even in the real-property context -- you know, we're not talking about homeowners, but a business property. When you open it up to the public, you don't have unfettered rights to exclude people for any reason, whatsoever.

And in fact Judge Posner, in the *Desnick versus American Broadcasting Companies* case -- and this case was not cited by anybody. I found it by Shepardizing one of their cases; the *Dietemann versus Time* case. It distinguished that. It's at 44 F. 3d. 1345, Seventh Circuit, 1995.

There was a case where ABC News fraudulently gained inducement into an eye clinic, in order to do an exposé, and then broadcast information about it.

And Judge Posner, under Illinois law, said, you know, in the context of business property that's been open to the public, we have to be careful about other policy considerations on trespass, and that the objectives of trespass law are to protect breach of peace, invasion of privacy, damage to property. And none of these things exist, because -- he went through each of the factors in the case, and said there was no breach of the peace, no disruption of the business, no damage to property, no invasion of privacy. And therefore, why would

you apply trespass law to -- to access to a business property that doesn't fulfill any of the purposes that trespass was enacted to address?

So I think to interpret a 500 million-member website open to billions of people on the World Wide Web -- to say that they can single out somebody that they don't like, because they're using information for a commercial purpose, ban them from the site, from gaining public information that anyone else in the world can get, and then say that's criminal -- and, by the way, not just if you're doing it by automated bots, but under their interpretation, if I got one of those letters, and I typed their website address in again, I'm a criminal, even if I just look at it, whether I manually copy it --

THE COURT: You disagree with Judge Breyer, I take it, in the *3Taps* case?

MR. WISOFF: I do disagree with Judge Breyer, although I do think that this case was different than this case.

And I think that their own privacy policies don't support their argument. And I think when they choose California law as the law to govern their dispute under their User Agreement, that it's a little bit hypocritical to come to court and say that California's law is preëmpted.

MR. VERILLI: Your Honor, may I have a few words?

THE COURT: Yes, you --

MR. VERILLI: Thank you, Your Honor.

MR. WISOFF: Your Honor --

MR. VERILLI: Thank you, Your Honor.

THE COURT: I've got to move on.

MR. GUPTA: Okay. Thank you. I just wanted to let you know that Professor Tribe would also like to speak.

THE COURT: All right. So we're going to move on.

MR. VERILLI: A few points.

Your Honor's identified Judge Breyer's opinion. And, of course, Judge Breyer noted the very statute at issue in the very next subsection draws a distinction between public and nonpublic computers. It doesn't draw that distinction in the preceding subsection, the one that's applicable to our case. So Congress knew how to draw the line; didn't draw it.

Second, with respect to the consequences of adopting the position my friend on the other side is urging, they kind of spun up a lot of smoke about how there won't be a lot of adverse consequences, but of course, there would, because their argument is that unless we've got a wall, and this information is password protected, that we can't assert a CFAA right against anyone. So it means not just that we can't assert it against them. We can't assert it against identity thieves, scammers, spammers -- you name it -- because it's not behind a wall. That's their argument.

And I think the consequences of adopting a position like

that in the absence of any statutory authority -- a Ninth Circuit authority, interpreting the statute pointing exact opposite direction would be extraordinary.

THE COURT: Well, what do you mean: You can't assert? If a hacker gets in, and breaches, and goes beyond just whatever the surface is that's visibly visible to the public, obviously, you have to -- a hacker would have to get in there and get information that is not public, but private --

MR. VIRELLI: But Your Honor has made a point already, though, that --

THE COURT: -- the CFAA would --

MR. VIRELLI: These bots are hitting us 95 million times a day. We don't know what they are in advance. But under their theory, we can't assert a CFAA against anybody.

THE COURT: You could use bots. You could employ self-help measures. That doesn't mean that then you can then enjoin the force of criminal law for somebody who defeats that bot, unless they get into the deeper layer.

MR. VERILLI: But then people who scrape for these other -- they say, *Well, we're scraping for this beneficial purpose*. Of course, we can test that.

But people who just scrape for nefarious purposes -- we can't use -- we can't invoke the CFAA against them. That's their position.

THE COURT: Well, if it's for nefarious purposes, you

may have a UCL claim. You may have a tort claim. You may have other statutes.

MR. VERILLI: Well, we may or we may not; but congress gave us this. And it does, by its plain terms, cover. The Ninth Circuit covers it.

If I could, before we move on to the constitutional issue -- and I know we're taxing Your Honor's patience -- there's one really important point. My friends on the other side have been saying this over and over and over again. It just isn't right. They've premised their whole case on this argument that once the information is visible, that it's public, and that we have made it available to everyone, without conditions. And that just isn't right.

It's wrong in a number of ways that we've already discussed. There are multiple conditions that are imposed. Do Not Broadcast is one condition. The prohibition on scraping is one condition. The fact that we put these technical measures in place to block is one condition.

And it gets to a point that I think is just of fundamental importance here, and it's this. Public/nonpublic is not an on/off switch. That isn't how it works. Routinely information is made public, but subject to conditions. And I'll try to give a couple of commonsense analogies that I hope will go straight to the point.

Take a public library. A public library makes the

information publicly available. You go and get books and other information and material from the public library, but the fact that the information's available to the public in that sense doesn't mean that you can break into the library with a crowbar at 2:00 in the morning, because you're seized in with a desire to read Moby Dick. It doesn't mean that you can take a book out, when you're supposed to return it in two weeks, and keep it for a year, because you want that information. It doesn't mean if your library privileges have been revoked for abusing the rules, that you can show a fake ID at the door, to get back in. The information's public, but it's subject to conditions.

Same thing with a museum. Works of art are made available to the public for viewing. That doesn't mean that the museum can't impose conditions. You can't take flash photographs. Maybe you can't take photographs, at all. Maybe you've got to pay for admission. You've got, you know, a whole set of conditions that are imposed on the public access.

THE COURT: What if the museum had an outdoor display in the public square? Took it outside. A sculpture, or whatever it is. And they said, *Well, you're in a public square. It's a public place. You can see it's open to all*, but then said, *No photographs*.

Now, would that be trespass, if someone came up -- it's on public land -- and took a photo?

MR. VERILLI: If there was a reasonable time. It's

the government, of course. The First Amendment applies to them, which isn't us, because we're a private entity, and the First Amendment doesn't apply to us; but with respect to the government, the question there would be whether it's a reasonable time, place, and manner restriction. And it might be.

THE COURT: But I'm wondering about trespass law. I mean, governments can enforce trespass laws, as well.

MR. VERILLI: Sure.

THE COURT: Would that be trespass, to take a photo, even though you're standing in a place that you're otherwise able to do, but you're doing something --

MR. VERILLI: Well, I don't know if that would be trespass, but here's what would I think, Your Honor. If somebody were taking a photograph, and were told that they weren't allowed to take a photograph, and they took another photograph, and they were told that they have to leave the premises because they're violating the rules, and then they left the premises, and they came back on, in violation of the order to leave the premises for violating rules, that would be trespass.

And that would be a case very much like *Virginia against Hicks*, which I know -- I assume we'll get to when we talk about the First Amendment. But that would be trespass here -- there. And that is effectively what we have here, Your Honor.

We've -- you know, they talk about how we connect up our servers to the Internet, and that means this information is available to the public. And that means, they say, that we can't impose any conditions on the availability of that information, because it's out there, and it's available to the public.

Well, there's just --

THE COURT: Well, it's not that you can't impose conditions. The question is whether you can back up those conditions with the -- with the force of federal criminal law.

You may be able to back it up with state law, maybe some state trespass law, maybe common law, or just self-help for no legal remedy on the other side, which is one of the things we're going to talk about. But the question is whether you can criminalize violation of those conditions.

MR. VERILLI: So I'm going to repeat myself, and I apologize for doing so, but Congress has made the judgment in plain terms of Section 1030(a)(2), and it's made another judgment in plain terms later in the statute, that we can get a private right of action to enforce to enforce our ability to impose conditions that can control access. And it's just right there on the plain -- on the face of the statute. It's why Judge Breyer reached the result he reached.

And I would submit to Your Honor that that is actually the answer that is the speech-promoting answer in this case,

because the other options for us -- if my friends on the other side are right about the CFAA, either we've got to put up a wall and put everything behind a password, which means the information is not going to be publicly available anymore, which reduces the flow of the information to the public, or we're going to tell our members that they're vulnerable to this kind of surveillance and disclosure to their employers in a way that's certainly going to deter people from making that information available and visible to the public.

And so I really think, Your Honor, it's not just -- it's clear that we do have a clear right under the law. We do have a clear right, as the Ninth Circuit has interpreted the law. We are a private entity. These are our computer servers. The information resides on our servers. We have a right to control who gets access to it and who doesn't, because we're a private entity making private judgments. And our view of the law is the view of the law that is going to maximize the free flow of information.

THE COURT: All right.

MR. GUPTA: Your Honor, I'd like to hand it off to Professor Tribe, to talk about the constitutional avoidance issue here.

THE COURT: All right.

MR. TRIBE: Thank you, Your Honor.

THE COURT: Okay.

MR. TRIBE: Maybe I could begin with that library analogy before I try to put the case in its First Amendment setting. If it's a public library, you know, when I was a kid, the books used to have a little tag inside that would tell you how often the book was taken out, and when.

And I think when the public library lets people take those books home, if they manually write down, *The most popular books are the ones in the geography section* -- not likely, but suppose it was -- and I want to make use of that information, for the government to make it a crime for me to make use of that information because they want to be the, perhaps, exclusive distributors of information about what's popular to read would, of course, be unconstitutional.

That's the setting in which I want to put this case.

Orin Kerr's article was very convincing to me, partly because in 1991 I wrote pretty much the same thing in an article called, "The Constitution in Cyberspace." It is ridiculous in today's world to use concepts like physical trespass when you're talking about the public pages of a website.

And it's not only ridiculous. There is authority on the point. In *Packingham against North Carolina* on the 19th of June this year the Supreme Court very clearly said that public websites -- and they used LinkedIn as an example -- are public fora. They are the current equivalent of the town square, to

use Your Honor's analogy.

Now, that doesn't mean that for all purposes, social media are to be treated as public utilities. I mean, all of the cases that they cited in their brief -- *Quigley*, *Buza*, *Langdon*, *Kinderstart*, *Howard*, *Green*; cases about how Yahoo! and Google and AOL are not simply public utilities; they have a right to exercise editorial control. Those have nothing do with this case. We are not arguing that we have some right to convert LinkedIn's pages to our own purposes. We're not trying to post things on LinkedIn.

We're simply trying to do what the public, as a whole, has been invited to do; and that is observe, collate the information, use data science to process it and make it more useful, both to employers who want to retain those of their employees who are apparently most desirable to the outside world, and outside employers who want to give employees greater opportunity.

So *Packingham* holds that for that purpose, social media are the modern equivalent of the town square. And it also holds -- and this is really important, I think -- that a content-neutral restriction --

And in part three of the *Packingham* opinion, the Court said that for purposes of this opinion, we will assume that it's content neutral when you tell sex predators that they cannot use any social media.

-- that a content-neutral restriction of First Amendment activity is subject to intermediate scrutiny and a narrow tailoring requirement.

And so, of course, if they do have interests, like not being overwhelmed by an army of bots that lead them to go -- you know, their servers to crash. If they can show when this case gets beyond the preliminary stage, before they put us out of business -- if they can show that they are using the narrowest-possible alternative to serve that legitimate interest, then we would have a different case. Perhaps the First Amendment standard could be met.

THE COURT: But that would suggest that every organization that puts themselves out on the Internet, to the extent they want to limit bots or some other kind of -- you know, put some technological "speed bumps," as Orin Kerr puts it, that would be subject to constitutional scrutiny, intermediate scrutiny, a narrowly tailored view. And wouldn't be that a pretty profound burden placed on even small websites or small businesses, that don't have the ability to -- they just buy off-the-shelf packages, that software anti-hacking stuff, that may be overly broad in terms of who it filters out, and the barriers that it imposes? Would they have to go through a narrowly tailored constitutional review every time anybody --

MR. TRIBE: Well, not strict scrutiny. "Narrowly

tailored" simply means they have to show that it is not gratuitously and substantially overbroad. That's not a burden, after ***Ward v. Rock for Racism*** [sic]. That's not a burden that the Court has thought to be too extreme.

But look at how extreme their position is, when a website that has tens of millions, hundreds of millions of people who put their profiles out there to reach as much of the world as they can is allowed to say, *You know, your business model is pretty good. We've been visiting your seminars. Now we want to adopt it, and kick you off.*

Well, that can't be done, unless you accept their position that this case has nothing do with the First Amendment, because we're not talking about protest or dissent. We've got a serious problem that follows from their position.

And in the *Sorrell* case the Court made very clear -- *Sorrell v. IMS Health* -- by a vote of six to three that data mining of information whose owner has put it out to the world, as the doctors in Vermont did when they said that *It's okay for you to look at our prescription practices* -- that that kind of data mining for purposes of marketing to those who could use the analyzed information to make sounder economic decisions is fully protected free speech.

Now, what make this case particularly dramatic, as Your Honor noted, is that they're putting in the hands of a private entity. And they emphasize how private LinkedIn is. It's not

the city. It's not the town. True enough. But that just make this a more extreme First Amendment violation, because they want to delegate -- they want to read the CFAA as though Congress, in its wisdom, decided to delegate to any website, however huge, the unilateral, unrestrained discretion to decide whom to lock out and deauthorize, for whatever reason, whether 2they don't want the competition, or whether they have objections to the race, or the religion, or the sexual orientation of the owner.

That violates a core principle that's been adopted by the Supreme Court, even when the power is delegated to a responsible governmental entity. Think of a case like --

THE COURT: But that's the question; is it?

MR. TRIBE: Mm-hm.

THE COURT: Where is the state action?

Because all of the other cases, whether it's *Sorrell*, or *Packingham*, there are obvious state actions. It's not a problem.

Here are you relying on some delegation?

MR. TRIBE: Yes.

THE COURT: Because it's not -- you can't say this is a case where they're -- like a railroad case, where there's active encouragement. By regulations, railroads were forced to engage in your analysis.

You don't have -- the CFAA doesn't force them to do that.

It gives them --

MR. TRIBE: No. They're simply handing a blank check.

THE COURT: Okay. And those cases where there's delegation usually involve a delegation of inherently sovereign power; something that's traditionally within the sovereignty, within the power of the government.

Here, running a business -- I mean, I could understand why it's like the town square in a functional way, but I don't understand why it is state action.

MR. TRIBE: Well, take a case like *Marsh against Alabama*. In *Marsh*, it was a privately owned company town in Chickasaw. And that company town was given the power under Alabama law to call the police, and have anybody who comes into the town to distribute literature that they don't want distributed, or for any other purpose, to call the police, arrest them for trespass, prosecute them, and convict them.

This is like *Marsh*. Now, *Marsh* held that deciding who can use the public parts of the town is an inherently governmental function. And it seems to me that after *Packingham* deciding who can visit the public site of something like LinkedIn is exactly like deciding who can use the public parks and streets of a town. That analogy is not --

THE COURT: That was barring -- but there, that was action barring offenders from the entire -- essentially, the

entire Internet; not from visiting a particular site.

MR. TRIBE: Well, the Court did say in the Kennedy opinion that if you exclude someone from websites like -- and it used the examples of Twitter, LinkedIn, and Facebook -- that you're excluding them from the equivalent of the modern town square.

They didn't say you have to exclude from all media; that is, if there had been a modification of the North Carolina law in *Packingham*, saying that a certain group of people -- and it's hard to think of a group less sympathetic and more dangerous than registered sex offenders -- that they can't visit a social platform that has on it the profiles and professional aspirations of a substantial percentage of the world, the case wouldn't have come out differently. It was not a quantitative case. It was a case about principle.

And when the Court has said in cases like *Lakewood against Plain Dealer*, in 1988, which involved a delegation by law to a town of the power to decide which news boxes may or may not be attached to public utility poles, the Court said that even if the right to attach something to a public property is not directly protected by the First Amendment, the danger of giving even a town, let alone a private entity -- a huge, powerful private entity -- discretion to decide who may and who may not engage in activity that is related to freedom of speech and information is constitutionally impermissible.

THE COURT: That was speech on public property.

MR. TRIBE: That's correct. And this is --

THE COURT: Well, you would say *Packingham* makes it public property -- makes the Internet public property.

I'm not quite sure it goes that far.

MR. TRIBE: Well, it does say it's the modern equivalent of the town square.

The real reason that this is so crucial, Your Honor, is that the First Amendment has really two branches. There's a branch that directly deals with government censorship. It says that if the government, itself, uses forbidden criteria, that's no good, unless it's overwhelmingly justified.

Then there's another branch that says that there must be enough breathing room for speech; that is, if you could divide up the world -- either the cyberworld or the physical world -- into privately owned enclaves, where people who want to engage in information processing or the dissemination of ideas need the permission of the private owner, then there isn't enough breathing room. That's where the public forum doctrine was born.

And what the Court said last month was that in today's world, for there to be enough breathing room, you have to treat privately owned social media platforms, at least in their public face, as public forums. And it seems to me that that First Amendment principle is what's crucial here.

In our brief, I cited the *Grendel's Den* case, which happens to be a favorite of mine because it arose in Cambridge, and I was involved from the very beginning. It was a case that served for the same principle. A body as private as a church cannot be given governmental power over First Amendment activity by state law. It also can't be given that power by federal law.

Now, Your Honor was certainly right that the federal statute trumps contrary state law, although I agree with my colleague that because the federal statute, the CFAA, doesn't lay out detailed criteria for what constitutes authorization or revocation, that there's room to absorb -- and there's a presumption that one should absorb -- the backgrounds body of state law in which the federal law is immersed; but surely the federal statute trumps even a state constitutional provision, which is one of the sources of our affirmative right here in the *PruneYard* decision; but what trumps the federal statute is surely the U.S. Constitution.

And I submit that even without deciding, especially at this preliminary stage, that it would clearly violate the First Amendment to read the CFAA the way my friend Verilli wants to read it, it surely raises a grave constitutional question that could be best avoided by deciding that this language about authorization, which does not look to me unambiguous in today's world, at least, as applied to the public pages of a website

like LinkedIn, reading that word "authorization" gratuitously to completely wipe out the free-speech use that an organization like hiQ wishes to make of that website seems to me to be creating a constitutional problem that Your Honor would want to avoid; that is, you want to construe the CFAA and the California Penal Code not to clearly give this owner the unilateral power, unbridled, to decide whom to admit and whom not to admit; that is, they were fine with what we were doing, until it looked like we could make money from it, and then they thought, *Hey, there's an opportunity for us*, which is why we're suing under the Unfair Competition Law.

THE COURT: So is your First Amendment argument that the First Amendment applies to anyone who participates now in this newly declared public forum -- i.e., the Internet -- and that would apply not just to LinkedIn, but any small website. any business? They would still be subject to scrutiny, in terms of whether they could disable or disallow/deauthorize people from accessing the website?

Or is it more the fact that the CFAA has delegated essentially a sovereign power now, and that the deployment of the CFAA would implicate the First Amendment?

MR. TRIBE: It's principally the latter, but it's also in part the former, in the sense that if you look back at the series of decisions that ultimately led to *PruneYard*, the Court seemed to draw a quantitative distinction. A large

shopping center opened to the general public in California is subject to the Free Speech Clause of the State Constitution.

It doesn't mean that a mom-and-pop grocery store has to allow people who enter the store to circulate petitions; that is, there may be a kind of de minimis exception before something is classified as fitting the model of a social media platform in the modern age.

But surely Your Honor needn't solve all of those problems at this stage. That is one of the, I think, sound pieces of advice that Justice Kennedy gave in the ***Packingham*** case, was that we should tread carefully before withdrawing First Amendment protection from anything as important as a social media platform of great magnitude.

Now, my friends turn that around, and say that being cautious means we should put you out of business, because in the long run if there are too many guys like you, we might get overrun.

Well, in the long run we're all dead, but I think we can cross that bridge we when come to it. And I don't think that they've made case of any kind for suffocating the First Amendment in this sweeping way at this stage.

One thing I want to say that is not directly related to the First Amendment. I was interested in the argument that we could always go elsewhere. You know, if we're kicked off of LinkedIn, we can go somewhere else. And I was thinking of

Whac-A-Mole. I mean, if LinkedIn has this power, so does Facebook; and the entire universe of cyberspace can be gobbled up by a small number of private owners. That can't be what the law of an open, democratic society with the First Amendment means. It can't possibly mean that.

And what we suggest is that at least keeping us alive to fight another day, when we face these difficult issues of *What are the less-restrictive alternatives? What are the more narrowly tailored alternatives*, is the right way to solve the problem.

It's certainly not the case, as my friend Mr. Verilli suggests, that the Ninth Circuit has already ended this inquiry in *Nosal II*, and in a number of other --

THE COURT: *Power Ventures*. Yeah.

MR. TRIBE: I mean, they -- it -- clearly, this concern about free speech was not central in those cases. Those cases involved using false pretenses or inducing people to let you pass a password.

This case is about the public space. "Public" means "public."

And it seems to me that when Mr. Wisoff talked about the Fourth Amendment law of justifiable expectations of privacy, he brought the case home in an important way; that is, if you say *I want my stuff to be public* --

And I really liked your question whether they have an

option for saying, *I want it to be as public as possible. I want Broadcast*.

-- then it seems to me you're not respecting personal autonomy by creating an automatic ability on the part of the owner of the website, not the individual, to simply choose, for whatever reason, however anticompetitive or otherwise difficult, to knock someone off the website.

And I think that no matter how many times they use adjectives like "scraping" and make it sound like we're engaging in some kind of predatory behavior, they're really not making what I would regard as a legal point that answers *Packingham* and *Sorrell* and the cases about impermissible delegation of power to criminalize, *Marsh*, *Grendel's Den*, which involved de-licensing, and not even criminalization, and other cases that stand for the broad proposition that giving any powerful entity, public or private, the ability to choke off, at its discretion, speech and the precursor of speech, the analysis of information, and the gathering of facts in the decision of how to make them most useful, is a dangerous path down which we should not go.

THE COURT: All right. Thank you, Professor.

MR. TRIBE: Thank you, Your Honor.

THE COURT: Let me give Mr. Verilli a chance to respond.

MR. VERRILLI: Thank you, Your Honor. I'd like to

first talk about the nature of the law being enforced here, and the nature of the right that we're asserting, and why it demonstrates there's no First Amendment issue. Then I want to address the delegation point that Professor Tribe has focused most of his energies on. And then I want to also talk about the *Packingham* decision in particular, and this question about whether constitutional avoidance is probative.

So let me start with the nature of the law. As the Ninth Circuit said in *Power Ventures*, the CFAA is a computer trespass law. It applies to prohibit or provide a private cause of action against unauthorized access to private computers, no matter why the entity wants to gain that unauthorized access, whether they want to do it to harvest data that they can subsequently use to support speech activity, whether they want to do it in order to engage in identity theft, or in order to do a denial-of service attack. Doesn't matter why. The law does not turn on the motive of the person seeking unauthorized access. In that regard, it is a classic law of general application that is not subject to any First Amendment scrutiny when it is enforced.

That's what *Virginia against Hicks* says, by the Supreme Court*; Cohen against Cowles Media*. That's a fundamental principle of Supreme Court First Amendment jurisprudence, that when a law is a law of general application that applies irrespective of any connection or lack of connection to speech

activity, there is no First Amendment argument to be made.

Secondly --

THE COURT: Well, isn't there a converse implication that's troubling? Maybe it's not a First Amendment problem, but what about hiQ's argument that if you arm LinkedIn and other large websites with a power to deauthorize and debar or demit large classes of people, even, let's say, on the basis of race, gender, political beliefs, competition, it seems to me that you're saying, *Well, the law is a law. And it's like trespass law: You can bar anybody you want for any reason, even if it's the kind of thing that would implicate traditional First Amendment concerns, to exclude people from a particular website, particularly if it's for information gathering*.

Isn't that troubling?

MR. VERILLI: So a few points about that. First, of course, LinkedIn doesn't do that, and that's not what this case is about.

THE COURT: But I have to think about what your proffered interpretation of the CFAA is.

MR. VERILLI: Of course.

THE COURT: Once you withdraw authorization, even with a simple cease-and-desist letter, without any technology, that's it. You can't even look at the website -- whoever the recipient is.

MR. VERILLI: Yes. There's another important

qualification to the applicability of the statute, which is that the incursion has to inflict a minimum of $5,000 worth of damage. And that's going to take out of the equation the vast majority of the circumstances that are in the parade of horribles that my friends on the other side have identified.

With respect to a class of people defined by race or religion, for example, there's no way that anybody's going to be able to go through and say for each and every one of them their use of the website is inflicting $5,000 worth of damages on us. So as a practical matter at a very minimum, those cases are never going to come up.

And, of course, the CFAA has been around a long time. And those case versus never come up because they don't occur. People don't do that. And what my friends on the other side are suggesting is that on the basis of this kind of far-fetched hypothetical that never comes up in the real world, that the statute contains a practical -- a practical mechanism to deal with anyway, that you should interpret the statute so as not to apply to this kind of situation that doesn't present any of those concerns, and does present a kind of concern that the statute exists to address. And, you know --

But the second point with respect to going back to basic First Amendment doctrine that I think is critical here is that the incursion -- the unauthorized access here -- is not, itself, speech. It's gathering data to support speech in the

future; but it's not, itself, speech.

So the statute is not regulating expressive activity. It isn't doing that. It's regulating nonexpressive conduct. It's not speech, itself. And it's not conduct that has an inherent expressive element, like burning a draft card or burning a flag, in which case --

THE COURT: Well, the gathering -- I understand your argument about, *You have to have one of them speak here, or you have the right to receive information*. So I don't think you're going to have to spend a lot of time on that.

MR. VERILLI: Yeah.

THE COURT: But I don't know if I buy the argument that, well, just gathering information, harvesting information has no protection under the First Amendment of the Constitution. Maybe it's not expressive conduct, but it is the right to receive information, assuming other requisites are made.

MR. VERILLI: Right, but Your Honor, the other requisites are what is critical here. And there is no case ever that we've found or that our friends on the other side have cited that suggests that any right to receive information authorizes trespass, or authorizes a violation of any other legal norm that would otherwise prohibit the conduct.

And that gets back to this idea that it's a law of general application that prohibits trespass. And I don't know.

THE COURT: That begs the question. Trespass is somebody who wants to go into do that marketplace and actually get the books, or look at the art, or whatever it is. And so, I mean, it begs the question. The trespass is getting access to that information. I wonder if there can be trespass if they don't have a -- it's not trespass -- I mean, they're tied up.

MR. VERILLI: The problem, Your Honor, is that they're only tied up if you assume that we're the equivalent of the government, but we're not. We're a private company. These are private computers, private servers.

THE COURT: No. I understand that. And that's why I asked the questions of Professor Tribe.

MR. VERILLI: That's why I think that it is trespass. That's the classic definition of trespass, is unauthorized invasion of property, of space.

And that is what the CFAA protects against, and provides a remedy for. And that's how the Ninth Circuit described it. That's a law of general application.

So it's just like *Virginia against Hicks*. And there, you know, the person said -- the person was barred from being in a public housing project. And the person said, *Well, I need to* -- and the person said, *I need to go on that public housing project to engage in a speech*. And that's the particular forum which is very important: Engaging in speech.

And what the Supreme Court held was, well, no. That law

on trespass is a law of general application, and bars you, irrespective of the reason you want to go on the property.

And there, unlike here, they wanted to go on the property and actually engage in speech, which, of course, was what *PruneYard* was. *PruneYard* was not going into private property to gather data to use at a subsequent time. It was to engage in speech, itself, in that forum.

And so I think those two points, and then, in addition, the idea that even if you're going to take this gigantic leap, and treat us as though we were the government, and subject to a similar set of rules, this is clearly a reasonable time, place, and manner restriction, for all of the reasons we identified before. We have to have the ability to keep these bots out, and do our best to keep these bots out. And it can't be that first there's a First Amendment right to overcome that.

Now, if I might move on to the second point about the delegation, there's a dispositive difference between the situation here -- the sending the cease-and-desist letter -- and every single example that Professor Tribe has identified. In every single example he's identified, the private actor is exercising the government power, itself.

Grendel's Den is a good example. The church got to decide how the zoning laws were going to apply, and the church had the last word. There was no subsequent governmental body reviewing it. The government turned the decision over to the church, and

the church made the final decision.

Marsh against Alabama. *Marsh against Alabama*, the government basically turned everything over to the private company, and they got to make the final decision about how government power's exercised.

We sent a cease-and-desist letter. We are asserting our rights under the law, but we are not making the final decision. The final decision is up to a Court.

And so that's why there's state action in those cases, and not in this case.

And what I think my friend Professor Tribe is trying to address with his argument is that, well, yes, but you'll get to the decide as a private actor against whom you are going to assert your rights under the CFAA. And that's true, but that is a feature of trespass law generally. It is always the case that an entity that owns and controls property gets to decide who it's going allow access to, and who it isn't. And the courts routinely enforce trespass claims at civil law and in appropriate circumstances in criminal law, even though the root of the judgment about whether the law will be enforced is a decision of the property owner whether to allow access or not.

THE COURT: Well, that's where at least in California law *PruneYard* comes in, because the trespass law has been deemed at some point subject to some strictures of --

MR. VERRILLI: Yes. Certainly --

THE COURT: -- the right of expression under California.

MR. VERRILLI: -- true, but no one's taken the leap California case that we're aware of, Your Honor, to apply that to websites.

THE COURT: Well, the U.S. Supreme Court hasn't gone much further beyond *Marsh*.

MR. VERILLI: In fact, it's cut back on *Marsh* repeatedly --

THE COURT: I understand that.

MR. VERILLI: -- since the 1940s, when *Marsh* was enacted.

Now, if I might -- and that's why I think *Grendel's Den* and *Marsh* -- every case my friends on the other side have identified -- is a case in which the government has given the final word to a private party.

That's not this case. Right?

There's no case, I think, ever in history in which a cease-and-desist letter has been found to be state action. We certainly couldn't find one. Friends on the other side haven't identified one. And it would be an extraordinary thing to say that it is. It's a private assertion of rights. That's what it is. It isn't a state action. Can't be a state action.

Now with respect to the *Packingham* case and its

applicability or nonapplicability here, I want to make several points, if I could. First I direct Your Honor's attention to page 8 of the slip opinion. I apologize I don't have a more updated cite than that, but page 8 of the slip opinion, in which the case says exactly what Your Honor said it says. And in at least three places on page 8 what the Court said was that the fault of this North Carolina law is it's weak in its scope.

Even with these assumptions about the scope of the law that were set in the state's interest, the statute here enacts a prohibition unprecedented in the scope of the First Amendment speech it burdens. It bars access to, for many, one of the principal sources for knowing events, et cetera, et cetera. And, in sum, to foreclose access to social media altogether is to prevent the user to engage in a legitimate exercise of First Amendment rights.

There's no doubt that the scope was critical. And, in fact, the whole point of the case was that the scope was overbroad in relation to the state's interest in protecting minors, because it swept in a whole host of websites that didn't pose any risk of the sex offenders having contact with minors. So that's point one.

Point two. And I think Your Honor's identified this point exactly correctly, also. This was a state statute that was being enforced against an individual defendant. Obviously, there's state action there. And in that situation, you have

the state intervening in between an individual who wanted information, and the information that was out there to get.

That's nothing like this case.

In order to make *Packingham* like this case, what you'd have to -- you'd have to changes the facts, so that the sex offender would be making an argument.

So let's say you have a social media website that has -- that children use with great frequency, and that has a policy that says, *We're not allowing registered sex offenders to have access to this website*.

And the sex offender says, *Well, I have a First Amendment right to access to this website despite your denial of authorization, because that's information that is out there in the world, and you don't require a password, and so I can go on*. That would be the parallel to this case.

And it's -- and nothing that the Supreme Court said in *Packingham* comes anywhere near justifying that kind of a result. Nowhere near. And so with respect to *Packingham*, I think: Just not applicable.

With respect to *Sorrell*, of course, the key difference there was that the information at issue was already in the possession of the people who wanted to use it for speech. There was no trespass. There was no unauthorized access. There was no breaking of the law to get the information. There was no going around technological measures. It was already in

their possession, A.

And, B, what the Court said in that circumstance was because the information was already in the possession of the people who want to use it for speech, and the law directly targets the speech activity and says, *You may not use this law for speech*, based on those two things, the First Amendment applies.

In those two critical respects, this case is the polar opposite. This is information that's not in their possession. And it's a law that prohibits unauthorized access, irrespective of whether the entity seeking the access wants to use the information for speech, or not. So it really doesn't have anything to do with the case.

THE COURT: All right. So we're going to have to wrap this up. And I'll let Professor Tribe rebut.

MR. TRIBE: I'll try to be very brief.

In *Sorrell* the information is not in the possession of the data miner, which was IMS; it was in the possession of somebody else. And the people who gave consent were the doctors who prescribed.

And here, people who give consent are the people who put their profiles on. The case is on all fours with *Sorrell*, because *Sorrell* holds that, just as Your Honor said, gathering information and processing it is not just some ancillary activity related to speech; it's at the heart of the First

Amendment. The first Amendment is not applicable only to handing out placards and petitions. It's applicable to processing and gathering information.

And as far as *Packingham* is concerned, it is true that the breadth of the thing was important, but the Court did say -- and this is on page 1737 of 137 S. Court -- that this APPLIES to social networking websites like Facebook, LinkedIn, and Twitter.

Now, it can't be the law that if you exclude somebody from one of those at a time, that's okay; and then you do it from the second, that's fine; and the third, that's fine; but in the end you've excluded from everyone.

And he hasn't really answered -- Mr. Verilli hasn't really answered the Whac-A-Mole point. If they can say "No" to us, so can Facebook, so can every other website.

And as far as the answer to the delegation point, it really does -- you know, maybe I can use the word *"chutzpah*" in court. To say that their cease-and-desist letter is reviewed by a Court, and that's what makes it different -- that's nonsense. The cease-and-desist letter is weaponized. In their view, it is given the automatic effect of excluding anyone they want to exclude, by virtue of the Computer Fraud and Abuse Act. So that's not a distinction. It's a distinction without a difference.

And then the final point he makes is, *Let's not worry*

about our ability to exclude people on invidious grounds like race or belief. It's never happened; but that's because this case hasn't come up yet. People haven't yet had the effrontery to say that something that they make open to the entire world -- they have the power, by virtue of some federal law designed to prevent trespass, which is not this -- by virtue of that law, they have the power to send a kind of letter of marque and reprisal, as the Constitution put it, to kind of mark someone as ineligible to gather information. That's a breathtaking claim. If that claim --

THE COURT: Probably in part because the response was that the CFAA has a jurisdictional requirement of certain amount of damages before it can be brought to bear; and therefore, that screens out the vast majority of these parade of horribles.

MR. TRIBE: If somebody said that no company that is owned by -- that has a majority/minority ownership can access this site, that would certainly exceed the $5,000. We're not talking about the use of the exclusionary cease-and-desist power in a bill of tender way, simply to pick on particular individuals. Maybe that wouldn't meet the threshold. We're talking about uses that could be employing a forbidden criterion causing lots of harm, with lots of money at stake. Seems to me that if you were to allow this, then it would multiply the number of such cases. And I think that to do that

in a preliminary stage would be terrible.

MR. WISOFF: Your Honor, if I can make --

THE COURT: Last quick word.

MR. WISOFF: -- quick comment. So first of all, Mr. Verilli said that the CFAA didn't turn on the motive of the person seeking access to the computer. I don't think that's really what our argument has been.

Our argument -- what we've -- to the extent motive feeds into this, I think what we've said is there's nothing in the CFAA, just like any trespass law that's enacted at the state level, to suggest that it was meant to not live in harmony with other laws of general application. And so maybe the motive of the person seeking the information may not matter; but at the end of the day there is room for you to interpret the CFAA in a way where, even if under where they have a legitimate right to refuse access, that if they're doing it for an improper purpose -- a purpose that would violate other law -- that maybe their right is limited, especially in the context of a public website. So I think that motive can play into it from that end.

They've also said -- when you asked them, *Well, what if you were trying to exclude people based on race or religion*, one of their responses is, *Well, we don't do that. We don't discriminate. You don't have to worry about that*. Well, that very argument was rejected in *Nosal I*, where the Ninth Circuit

said -- where the prosecutor said, *Well, we wouldn't bring those kinds of cases*. And the Court said, *No. We have to interpret the statute in a way that is reasonable, and that has limits on it, and not rely on the good faith of prosecutors*. And if the Ninth Circuit was saying, *You can't rely on the good faith of prosecutors*, you certainly can't rely on the good faith of a private web owner.

And then finally on the $5,000 damages -- that provision has been interpreted to be satisfied, which they've done in this case, to say, *Well, we spent more than $5,000 investigating just to figure out who you were*. That criteria could be satisfied in each and every case. That is no practical limit.

So if you were to interpret the statute the way they say, they're sending of a letter, even if you're just manually accessing, even if you've done nothing, for whatever reason, even if it's based on race, religion, anticompetitive concerns, anything, you commit a crime the second you type that website address back into your browser. That cannot be a reasonable interpretation of the statute.

MR. VERRILLI: Your Honor, I apologize.

THE COURT: One extra minute.

MR. VERILLI: I'm going to tax your patience here, but let me be clear. We're not saying that this statute can be used to authorize these kinds of discrimination. What we're

saying is that if it ever is, the Court can decide in that case whether there's an interpretation of the statute that is appropriately limited, such that it can't be enforced when its enforcement would involve the enforcement of something that is discriminatory on the basis of race or --

THE COURT: How can you find that in the statute? If I find "authorization" means whatever --

MR. VERILLI: Well, I don't think you can find it in the statute. I think you'd have to decide in that circumstance whether there might be an as-applied limit under the Constitution.

THE COURT: Under the Constitution?

MR. VERILLI: Yeah. In a different case --

THE COURT: What were the constitutional arguments? If it's private, you've argued there's no state action.

MR. VERILLI: Right. Well, we think it is, but I think if -- what I'm trying to stress here, Your Honor, is that that's is a very different case than this one. It doesn't pose that issue.

THE COURT: It's a different case, but one has to look at the consequences of any interpretation; what the implications are.

MR. VERILLI: You're definitely correct, Your Honor. But I guess what I would try to leave Your Honor with is this; that in a situation in which the interests that the statute

exists to protect are directly implicated, and none of these kinds of concerns are present, the Court can reserve for another day the question of what to do in a case in which those concerns are present. And that does not and should not lead the Court to the conclusion that the statute ought not to be enforced in a situation in which its fundamental policies are implicated.

MR. WISOFF: Well, I think those concerns have been raised, Your Honor.

THE COURT: I'm going to take the matter under submission. My question is: Right now, pending my decision on this, did the parties have a stipulation to keep the -- I guess there's kind of a stay in place.

MR. VERILLI: Yes. There's a standstill agreement in place.

(Reporter requests clarification.)

THE COURT: Standstill.

I appreciate the briefing and the argument. Obviously, it's been is superb. And it's a very interesting issue. I've got a feeling it's not going to end here, so I will work on this as quickly as I can, and get it out.

MR. TRIBE: Thank you, Your Honor.

MR. VERILLI: Thank you, Your Honor.

(At 4:28 p.m. the proceedings were adjourned.)

I certify that the foregoing is a correct transcript from the record of proceedings in the above-entitled matter.

July 28, 2017

Signature of Court Reporter/Transcriber Date

Lydia Zinn