Illustration by: Lincoln Agnew

How an Experimental Billion-Dollar Privacy Lawsuit Could Clobber Facebook

by Eriq Gardner
J

What if law enforcement was outsourced to class action attorneys? Don't imagine. It's happening as the Cambridge Analytica scandal becomes Mark Zuckerberg's legal nightmare.

Less than one week. That's all the time needed for Jay Edelson to swing into action in March and file suit upon splashy headlines that Cambridge Analytica had harvested data from tens of millions of Facebook users in the interest of swinging the 2016 presidential election in favor of Donald Trump. Edelson was hardly the only class-action lawyer rushing to allege a huge violation of trust on the part of the world's biggest social network. But not every attorney is known to be a corporate America bogeyman, notorious for picking fights with large and small companies over the seedier sides of online life, including surreptitious information collection and the hawking of personal data to occasionally shady third parties.

The Cambridge Analytica scandal gave the 45-year-old bespectacled attorney with a passing resemblance to Steve Jobs an opportunity to go to court with a new story of tech infidelity. One that begins in 2014, when a Russian-American working for Cambridge Analytica created a personality quiz app called *thisisyourdigitallife*. About 270,000 users downloaded the app. Cambridge Analytica parlayed its modest access to the lives of ordinary Facebook users and their family and friends into more and more information — enough to begin psychologically profiling American voters and then bombarding them with phony and real news.

And Facebook's role?

"This kind of mass data collection was not only allowed but encouraged by Facebook, which sought to keep developers building on its platform and provide companies with all the tools they need to influence and manipulate user behavior," states the March 23 lawsuit filed by Edelson. "That's because Facebook is not a social media company; it is the largest data-mining operation in existence."

Sharp words, but Edelson obviously wasn't alone in expressing that sentiment. In addition to the many lawsuits filed over Cambridge Analytica, lawmakers have expressed outrage that Facebook hasn't taken user privacy seriously enough. And millions of consumers have decided to ditch the platform. But Edelson's lawsuit is notable — and not just for what the complaint says and the prospect that Facebook may pay through its digital nose.

Rather, if Edelson pulls this suit off, he'll be doing so in a brazenly new way, the type of achievement that could attract imitators from the ranks of other attorneys currently struggling to hold companies liable for privacy breaches. That scenario, in turn, could spur federal digital privacy legislation in the new year that could become a headache for CEO Mark Zuckerberg.

What makes the Edelson lawsuit different is a name barely anyone knows: Kimberly Foxx, a state's attorney, the top prosecutor in Cook County, Illinois. Edelson is ostensibly representing the people of Illinois through Foxx on a claim that Facebook engaged in unfair and deceptive conduct. Or, stated another way, a government official has *outsourced* law enforcement to a class-action attorney.

Edelson, having now been given the role of a Special Assistant State's Attorney thanks to possessing the "required legal expertise," as a court order confirming his appointment put it, aims to punish Facebook for violating The Illinois Consumer Fraud and Deceptive Business Practices Act. It carries massive repercussions, including $50,000 in civil penalties per violation, injunctive relief and — if egregious circumstances call for it — a lost business license to operate in the state. That's right. Theoretically, Facebook could pay billions and be prohibited from offering its service in Illinois if it loses this lawsuit.

No wonder Facebook is desperate to avoid that outcome.

"[T]he case is being directed and financed by private attorneys with no accountability to the State or Illinois voters, pursuant to a contract of questionable validity that awards them a significant contingent interest in any recovery," wrote Facebook's lawyers in a bid to keep the case from being litigated in state court. (Indeed, Edelson will collect 20 percent of whatever he wins in the case.)

The ongoing fight over this lawsuit has caught the attention of other attorneys. "The Edelson firm has generated notoriety with some of its privacy cases," says litigator Robert Schwartz, of the Quinn Emanuel firm, who has defended privacy cases for big companies. "I don't typically agree with their positions. But on this one, on the standing issue, they appear to have done their homework."

What Edelson's case portends is politically connected plaintiffs' lawyers working hand in hand with local regulators and testing out new legislation coming from the progressive quarters of the nation. These sorts of partnerships, sure to raise constitutional

challenges, threaten to become disruptive to companies that once made disruption a key part of their own missions. That could well become the incentive for goliaths like Facebook to get behind new federal legislation if only to preempt states like Illinois and California taking an even more punitive approach to privacy breaches. Already, the tech lobby has begun its push. It's not out of generosity. The goal is to supersede what's happening stateside.

"There's a lot of debate over what federal privacy legislation will look like," says Allie Bohm, a privacy expert at Public Knowledge. "After Europe passed GDPR [General Data Protection Regulation], a lot of Americans took notice. California passed an imperfect privacy law. A lot of states are going to act. I think you're going to see companies begin to come to the table and movement toward comprehensive privacy legislation in 2019."

"Cambridge Analytica, that's what gets people's attention," says the self-confident Edelson. "But really it just unmasked Facebook's modus operandi. It's one of a thousand examples."

Mark Zuckerberg

Read More

Facebook's Mark Zuckerberg Calls Cambridge Analytica Data Scandal "A Major Breach of Trust"

***

Since word of Cambridge Analytica's activity spread nine months ago, Facebook has paid quite a price. The company has lost a third of its market value. Zuckerberg was called to testify in front of Congress, where he offered mea culpas and vague promises to do better. That hasn't stymied the backlash. According to a Pew Research poll from September, 42 percent of Facebook users say they've taken a break from checking the platform for a period of several weeks or more, while 26 percent say they have deleted the Facebook app from their mobile phones. Accordingly, Facebook has revised its growth forecast down to pretty much nothing for 2019 as investors continue to punish the company's stock.

Yet for all the hullabaloo generated by the Cambridge Analytica scandal, it's hardly clear that Facebook did anything illegal. Despite the buzz, there really was no "hack" or "data breach" in the traditional sense. What Facebook did in trafficking in data is not too different from what many digital companies do on a daily basis. That includes corporations in the entertainment sector like CBS and Hulu, whose streaming services collect massive data profiles on their users and sell advertisers on the ability to target specific consumers.

It would also be wrong to assume that companies don't give a damn about protecting their customers' most sensitive

information. It's just that privacy is one of many interests. Sometimes there are trade-offs when deciding which aspects of a platform should be free and which should be subsidized by sponsors, which facets should be closed and which should be open enough to allow integration and apps built on top of the so-called social graph.

That was one of the points that Zuckerberg attempted to make to the U.S. Senate's Commerce and Judiciary committees back in April. "In 2007, we announced the Facebook developer platform, and the idea was that you wanted to make more experiences social, right?" Zuckerberg testified. "In order to do that, we needed to build a tool that allowed people to sign in to the app and bring some of their information, and some of their friends' information, to those apps. ... Now, a lot of good use cases came from that. I mean, there were games that were built. There were integrations with companies that, I think, we're familiar with, like Netflix and Spotify. But over time, what became clear was that that also enabled some abuse."

Facebook is hardly blameless, and its sins undoubtedly go beyond a failure of policing the exploitation of data. Those include data-sharing agreements that reportedly allowed companies like Amazon and Sony to surreptitiously obtain users' names, emails and contact information and might have technically allowed other companies including Netflix and Spotify to read users' private messages (even if there is no evidence that this actually happened or even that Facebook's partners were aware of such powers). And some of Facebook's activity arguably violated the company's 2011 agreement with the Federal Trade Commission in which the company pledged to

get consent from users before sharing their data with third parties.

Why hasn't the FTC done anything?

"The FTC is extraordinarily understaffed and under-resourced," says Bohm. "The FTC would have to go to court, but they have just 60 technologists nationwide. It is a really small number."

As for private citizens taking Facebook to court, it's not so easy.

First, users consent to all sorts of broad data collection and sharing as a condition of using the platform in the Terms of Service, the fine print that users click assent to often without reading. That clickwrap agreement also designates that any disputes go to a federal court in Northern California — Facebook's home turf (although that's more generous than the way most digital companies force aggrieved users into arbitration and forgo participation in a class action).

The next challenge for anyone wishing to sue is that there's only a patchwork of privacy laws that would provide grounds. Most of these laws are sector-specific (e.g., statutes covering health records or students' education records), narrowly and confusingly drawn up (e.g., the Video Privacy Protection Act, which prevents a tape service provider from knowingly disclosing personally identifiable information), or can be defeated by a showing of consent or no reasonable expectation of privacy (e.g. wiretapping laws).

Finally, merely identifying the relevant broken law is not enough. Thanks to some recent jurisprudence — in particular, the 2016 U.S. Supreme Court decision in *Spokeo v. Robins* — privacy

plaintiffs in federal court must show an injury is real, not abstract, and harm both "concrete and particularized." Otherwise, these plaintiffs have no standing to pursue their claims.

How does that work? Well, the Cambridge Analytica scandal provides a working example. In fact, in the months that followed Zuckerberg's tour of contrition before lawmakers and reporters, Facebook's lawyers were consolidating all of the class actions brought over the Cambridge Analytica affair into one giant case in San Francisco.

And then Facebook attacked.

In a motion to dismiss, Facebook ridiculed the theories of harm, which ranged from drained cellphone batteries to the election of President Trump. The company's lawyers pointed out that the alleged victims hadn't described any specific content shared or illicitly obtained by third parties. Facebook alluded to how some users may not have adjusted their privacy settings to opt out of sharing. "Nor do Plaintiffs explain how the Cambridge Analytica events or the alleged sharing of data with any third-party apps or device makers led them, personally, to suffer any cognizable injury," continued the court brief. "Indeed, they do not explain how the alleged conduct ... caused injury to any Facebook users — only that it supposedly led to some users being served more tailored ads and enabled some users to use Facebook on their mobile devices, neither of which is 'harm' at all."

In other words, Facebook's lawyers argued, what's the fuss?

But one group of consumers may or may not be part of this consolidated action in a San Francisco federal court. Those are

the Illinois citizens represented by Edelson and his colleagues, one of whom once told *The New York Times* of joining the firm because "it seemed like a private version of the FTC."

"The way that defendants deal with privacy cases is to try to get them kicked out on technical grounds so there is never any discovery," says Edelson. "So when they argue, 'There's no standing. There's no damages,' their goal is to never get to discovery. But when regulators bring suit, it's hard for them to have that silver bullet in the beginning."

Read More

Mark Zuckerberg Admits Facebook "Made Mistakes" Amid Massive Data Breach Scandal

***

The Chicago offices of Edelson's firm boast an indoor volleyball court, golf simulators, a pingpong table, a pool and a large mural of emcees in the midst of a rap battle, all of which is meant to get the competitive juices flowing for the more than 30 lawyers who work there. Then there's the law firm's group of computer forensic engineers, who can be seen on a regular basis fiddling with new tech devices and hot apps in an attempt to figure out the inner workings and potential privacy problems. Knowing his reputation as an antagonist of tech companies, he says, "What's ironic is that our culture is much like a startup culture."

It is from this office tower that Edelson has been fighting to get his latest case out of San Francisco and back into Illinois state court. The details of the competing legal arguments are wonky, but they deal with who is representing whom and grants of authority for purposes of establishing jurisdiction. They have the judge examining all sorts of issues related to the power of a low-level government official like Foxx, Illinois Attorney General Lisa Madigan and, of course, Edelson.

Edelson is accustomed to big cases that have lasting legacy. In fact, he was the attorney representing the plaintiff in *Spokeo v. Robins*, which dealt with a man who sued over a website that aggregated data for the purposes of showing interested parties

an individual’s "credit estimate" and "wealth level,” among other pieces of personal information. *Spokeo* highlighted the difficulties of establishing standing in federal court. Edelson notes, “The defense bar has spent my entire career trying to get every class action into federal court. ... They were very aggressive [in trying to] avoid state courts, which were supposedly more sympathetic to plaintiffs' claims.”

If the lawsuit over Cambridge Analytica's harvesting of data proceeds in federal court, he'll know what to expect. He's currently pursuing Facebook on another front — alleging in a separate case that the social media giant violated the Illinois Biometric Information Privacy Act, a first-in-the-nation state statute that governs the collection and storage of fingerprints, facial scans and other bodily identifiers. That suit, which claims Facebook broke the law through its system for identifying and tagging the individuals in pictures posted by its users, is currently before the 9th U.S. Circuit Court of Appeals. Rushing to support Facebook in that appeal is the U.S. Chamber of Commerce, which in an amicus brief argues the case "presents questions of exceptional significance" and attacks the notion of Facebook potentially being liable for "billions of dollars in damages despite the absence of any allegations of real-world harm to anyone."


Mark Zuckerberg entering his second day of testimony

Read More

Mark Zuckerberg Reveals His Data Was Shared in Cambridge Analytica Leak

Although Edelson has been involved in a number of big privacy cases over the years against the likes of Google, Amazon, Apple, and Netflix, this appears to be the first time he's acting on behalf of a state's attorney. He says he'll soon have more suits representing regulators in other states.

That itself is significant and could foreshadow what's ahead. After all, in the past decade, state AGs have become a lot more aggressive in court in the face of the federal government's action or inaction. During the Obama years, AGs in conservative states challenged Obamacare and policies designed to protect "Dreamers." Now in the Trump years, AGs in liberal states are challenging immigration crackdowns, the rollback of net neutrality and a host of other issues including, now, privacy.

"I've been saying for years that, by and large, privacy class actions have failed to compensate people," says Edelson. "There is a hole — and someone is going to fill it. That's going to be regulators. In the past, it's been federal regulators. The FTC. The FCC. But that's now shifting to state regulators. I think that's what you are going to see in 2019."

In researching legal precedent from around the nation, Facebook struggled to find analogous situations to Edelson's current complaint. That's not to say that the lawsuit, built in its own way on top of Facebook's social graph, is the very first of its kind.

The better assessment is that it's an example of a relatively novel approach to law enforcement and regulation that has *just* begun to generate chatter in legal circles. For example, a February 2017 paper titled "Pirates at the Parchment Gates" by Margaret Little at the Competitive Enterprise Institute, a libertarian think tank, noted that some state AGs had in recent years partnered with private lawyers on a contingency basis to launch courtroom attacks on energy companies in the interest of doing something about climate change. Little was critical, raising concerns that these outsourcing arrangements "result in the privatization of law enforcement, and thus transfer power into the hands of influential private counsel who have cashed in for billions of dollars in fees—in open defiance of constitutional and legal prohibitions put into place by our nation's Founders to prevent such corruption."

Little questioned whether the hiring of private lawyers to stand in the place of government officials and reap a significant portion of money that would otherwise be going to taxpayers amounted to an end run around legislative authority and violated the due process rights of its targets. Those concerns may one day come before the Supreme Court and its majority of conservative justices.

In the meantime, Facebook's privacy problem has at least *some* regulators taking action — albeit in different ways. A lawsuit filed Dec. 19 by the attorney general of Washington, D.C., against Facebook over the Cambridge Analytica scandal was hailed by some as the first, although that assessment ignored what one state's attorney in Cook County, Illinois, had authorized nine months back.


Facebook CEO Mark Zuckerberg

Read More

Mark Zuckerberg Does Damage Control Over N.Y. Times Exposé, Says He Has "Tremendous Respect" for George Soros

If Edelson's case against Facebook manages to navigate hurdles to score a huge settlement — after all, class actions rarely see trial — expect to see more cases now that states throughout the country are either passing or contemplating new laws on the privacy front. The Illinois Biometric Information Privacy Act is one example of such a law. (It was the result of an extensive lobbying back-and-forth between advocates such as the Digital Privacy Alliance, whose legislative director Jacob Wright is also an Edelson attorney, and The Illinois Chamber of Commerce, whose technology council is co-chaired by Facebook lobbyist Dan Sachs.)

Then there's California, which in June passed a new privacy law giving its citizens the right to know what personal information a business has collected about them, the right to "opt out" from businesses selling personal information to third parties, and the right to have a business delete their personal information. The requirements won't take effect until January 2020, however, and there's quite a few questions about implementation and enforcement. Just before Christmas, California AG Xavier Becerra announced six public forums to discuss further rulemaking. That may give digital companies the opportunity to soften the edges of the California privacy law. Many of those corporate interests only gave a lukewarm embrace of the California Consumer Privacy Act in the face of a ballot initiative that offered the prospect of even tougher oversight of technology companies.

But that's often how these things work. Legislation regulating business comes not simply because of public scandal. New laws and regulations appear because the alternative of doing nothing presents an even greater threat for business. Ballot initiatives, state legislatures and maybe class-action lawyers in the ears of public officials few know about could provide the stick that prods the digital industry to strongly request intervention at the federal level. Already, the Internet Association — whose membership includes the likes of Amazon, Spotify, Uber and yes, Facebook — put forward "principles" for such discussion in September. Among them is the proposition that a "national framework should specifically pre-empt the patchwork of different data breach notification laws in all 50 states and the District of Columbia to provide consistency for individuals and companies alike."

Until then, the threat of lawyers like Edelson looms.

"It's still too early to assume that Facebook skates by," says Santa Clara University School of Law professor Eric Goldman, who specializes in tech law. "There are thousands of regulators now looking to nail Facebook. That's before class-action lawyers, and states like California, unleashing another class of regulators on the company's home turf. We don't have the test results back."

A version of this story first appeared in the Jan. 9 issue of The Hollywood Reporter magazine. To receive the magazine, click here to subscribe.