PHAWKER
You Report, We Decide.

Q&A: With Online Privacy Expert Lori Andrews

January 12, 2012

The take away from *I Know Who You Are And Saw What You Did* is this: As an Internet user your rights are exactly none. Actually, that's not true, you do have the right not to use it. But assuming you have waived that right, know that you are being watched, probed and profiled, your footprints are being tracked from your front door to the furthest reaches of the digital ether and back. They know who you are and what you did. Somewhere there is a file being kept on you. They know a thousand things about you. Preferences, locations, affiliations. Your best hopes, your worst fears, your darkest desires. Data miners have been hoovering up your digital chem trails and selling them to marketers, corporations, employers, and law enforcement. Anything you say or do, can and will be used against you, according to legal expert Lori Andrews, author of *I Know Who You Are And Saw What You Did*.

Andrews is a law professor whose work assesses the social impact of emerging technologies. She directs the Institute for Science, Law and Technology at Illinois Institute of Technology, where she teaches a class on the Law of Social Networks. She is the author of 14 books. Her groundbreaking pro bono litigation caused the National Law Journal to list her as one of the 100 Most Influential Lawyers in America.

Andrews thinks the online world needs the kind of constitutional protections we enjoy in the offline world. If Facebook's 750,000,000 million people makes it the third largest nation in the world, she argues, it should have a constitution. She's even gone to the trouble of writing one. Tonight at the National Constitution Center, Andrews, along with Kashmir Hill, a blogger for Forbes, and New York

Times reporter Jennifer Preston will consider what the Constitution would look like if the Internet and social networking was around in the time of the Founding Fathers.

PHAWKER: For the benefit of the reader, explain the premise of your book.

LORI ANDREWS: The premise of my book, is that our online self has become more important than our physical self. One in five college admissions officers look at Facebook pages in deciding whether to admit students. Thirty-five percent of employers say they won't hire someone who's got pictures of themselves in provocative dress or with a wine glass on their Facebook page. And I advocate a constitution for social networks to make sure we have freedom of speech, privacy, the right to a fair trial—the sort of protections we have in the offline world.

PHAWKER: Do you get annoyed when the media calls you a "privacy advocate," like it's some sort of esoteric minority interest, like Marxism, or bestiality, or something?

LORI ANDREWS: I think that there are a lot of the people in the media who say people should know better than to post a drunken Facebook photo, and employers should have the right to that information, but pretty soon you can win those people over by pointing out that data aggregators are collecting information about them that they wouldn't want made public. There's a case going on in California right now, whereNebuAd, a marketing company, made a deal with service providers to put hardware on the Internet service providers network and actually collect every e-mail, every Skype call, every action that each user of the Internet in that locality made on the web and made deals to sell that information to advertisers. They might be pharmaceutical companies who want to advertise something because of a personal health comment that you made in an e-mail to a friend, or the Google search you did for a symptom, even though it might not have been about yourself, and third parties are offering that information to employers. They might not want to hire someone who has a medical condition that would cause the person to miss work five days a year. So, you might be denied opportunities based on information about you that you didn't know you were disclosing. So, pretty soon, I find the very media that thinks it's not about privacy, and about openness are panicking and asking me 'What can I do about this?"

PHAWKER: Playing devil's advocate here, if you would codify this into law, wouldn't that mean that anything that's on the Internet then becomes inadmissible in court?

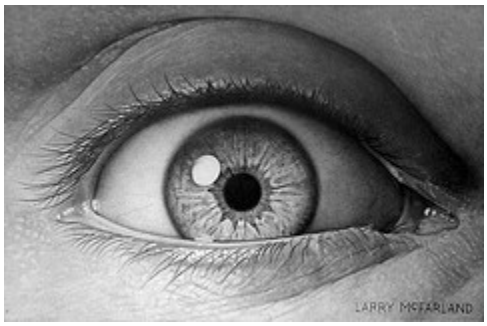
LORI ANDREWS: No, I actually think we should apply the world that we value offline, online. So, for example, we do have the right to a fair trial and so a women's past sexual history can't be admitted in rape cases. But now criminal courts are saying, "Well, let's admit the fact that she filled out a sex survey online, or that she has picture of an old boyfriend to try to undermine her creditability. Or women are losing custody of their kids, because they posted a sexy photo on Facebook, or because they say they "like" "National Weed Day." So, as opposed to other evidence, where there would be an actual investigation to see whether the child is safe or not, courts are admitting this without any view toward the usual rules of the game, of asking

whether it's relevant, or whether it's authentic, or related in some way to the case. And so people might see a few courts that have turned down this information. I remember one of them, the ex-wife was trying to have the children taken away from the ex-husband, because he published a picture of his new girlfriend in a French maid's costume, and also had a video of someone shooting Ronald McDonald in the face. Now we may all have different opinions about how appropriate that is, but it's pretty clear that you shouldn't take that as evidence that he's a bad dad.

PHAWKER: Are you telling me the Constitutional guarantees don't apply to anything online?

LORI ANDREWS: I'm saying that courts have thrown up their hands in a way that has not happened with other technologies. So I've worked in the past with medical technologies, genetic technologies, and forensic technologies, and all those instances, judges have been willing to apply fundamental concepts like privacy. With respect to the Internet and social networks, judges have erroneously failed to protect rights. And judges have said "an e-mail should be just like a postcard." So anything in an e-mail—the hotel I'm staying at now, or my credit card number—all that is public. Well, that doesn't make any sense, and it also doesn't comply with the offline rules.

PHAWKER: Could a reasonable case be made that the use of this information, as you're describing it, would be a violation of a defendant's or a litigant's Fourth Amendment rights?



LORI ANDREWS: Absolutely. I think a lot of it isn't about regulating the Internet per say, but regulating the native uses that are made of it. But so far, I've found case after case where this information is being used to prove a point where it doesn't necessarily stand for that. So, if you see a 7th grader making gang signs on a MySpace photo, right now, courts will say that it shows that he's a gang member. When in reality it could be that that he was bullied at school, and he's making gang signs to try to appear tougher than he is. So there's a way in which information is taken as truth by the courts. And now, we're even seeing people gaming the system, where the new girlfriend makes up a Facebook page in the name of the ex-wife, in order to help her husband win custody. So maybe it's that judges are less savvy about social networks, and are willing to take this evidence as truth, when it isn't necessarily.

PHAWKER: Is that an actual incident, where a girlfriend made a fake Facebook profile?

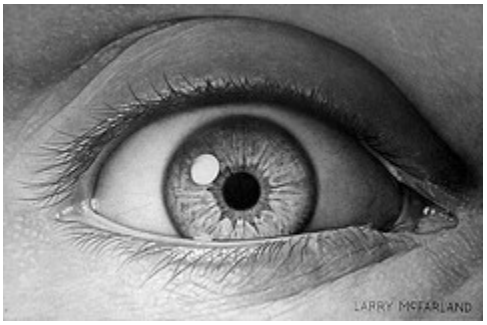
LORI ANDREWS: Yeah, those things happen. There was also an incident where kids get their penalties enhanced by wearing "gang colors" on their Facebook photos. I looked up the Los Angeles police department's definition of what "gang colors" are, and they include plaid—think of any hipster—or all black—think of any New York art opening. And so this information is being used inappropriately. It's intriguing to me, that the the defendants are beginning to fight

back, in subpoenaing the cops' Facebook and MySpace pages, and one defendant is being tried in possession of a gun in violation of his parole, actually used a cop's MySpace page setting of his mood as "Devious," to prove to the jury that the cop had planted the gun on him, even though, that emoticon might not actually indicate what the cop did, or didn't do. Fascinating, don't you think?

PHAWKER: Entirely. Are you one of these people who feel that the way we freely share personal information on social networks we're like the lobsters jumping into the pot?

LORI ANDREWS: I think that people don't realize that even seemingly innocuous photos, you having a glass of wine at a wedding, might be used against them, but it's also really tough, because the social networks keep changing the rules of the game. At first, Facebook promised everybody that all their information would be private. Then, Facebook made your friend's pictures public. So that might seem innocuous, but what happened was there were people in the U.S. who had friended people in Tehran, or had relatives in Tehran, and if the U.S. person posted something against the Iranian government, what happened was the now public pictures of friends were used to arrest and beat up family members and friends in Iran. So a very simple thing like all of a sudden making friend's pictures public could have huge ramifications. And yet, Facebook did that with a flip of the switch and not giving users adequate information, and so you might have seen that there was a recent settlement between the Federal Trade Commission and Facebook that requires Facebook to tell people when they're going to change the rules, and give people a chance not to be part of that more public approach. And a lot of people say, "Oh, privacy, let's just get over it," and that "it's a new era," that people don't care about privacy as much because look at all they post, but 65% of people do use Facebook privacy settings, and their concerns about privacy are even higher among younger people, who kind of get it, that they might lose a job or have other bad things happen to them, based on what they posted.

PHAWKER: Getting back to Facebook changing the rules all the time with very little notice—why is that? Why do they constantly make people feel like they are unwillingly in a game of three card monty with their private information?



LORI ANDREWS: I think the users of Facebook think they are the consumers, when they're actually the product. Facebook makes $1.86 billion a year through taking people's private information and making it available, and using it to target ads. So if I email a friend that I'm going to go on vaction in Florida, do a Google search about it, or post something about it on my Facebook page, that becomes information about me that can be marketed to, say, travel agencies, or local attractions in

Florida. And so, less privacy is always better for Facebook, because it gives them more information to sell. The more you say, the more they can track you through your friends, and the more, the better.

PHAWKER: We hear a lot about this data mining that you're talking about, that every consumer choice is being recorded somewhere. Does everybody in this country have a vast file being kept on them somewhere?

LORI ANDREWS: Well, there's one company that's called Axciom that has 1500 pieces of information on 96% of Americans. Their former CEO has called it "the biggest company you never heard of." They have everything from your political party, to whether you've ever taken drugs for incontinence. And some of the ways in which data aggregators get this information is by putting cookies, or web beacons, or flash cookies on your computer. And, amazingly, when consumers have gone to court and said "that marketing group should not be collecting information about me without my consent," courts have said it doesn't violate wire tap laws, or the Computer Fraud and Abuse Act, or any of these federal laws because the courts have said one party's consent is enough. And so if Facebook, or Amazon, or Dictionary.com says it's OK for a third party company to collect information about you—that's fine. The company doesn't have to ask you for your personal consent. And I think that's wrong—it's your information, they should have to ask you about collecting it.

And the most troubling thing that in California now, an ad company called NebuAd has made deals with Internet service providers to put hardware on the ISP's network to collect every transmission that every Internet user on that ISP makes. Every email, every Skype call, every search on the web. And what NebuAd said when they were sued for various privacy invasions, was that if we can't be liable under these federal laws because we have the ISP's consent, and therefore don't need the consumer's consent, how can we be liable under the state laws in California, which actually has a Constitutional privacy provision. Now that case will likely settle, and we won't have any precedent. But to me, that is amazing! When I go to make a purchase, when I put my social security number in to get a fishing license, or use my credit card to order a flight on Southwest Airlines, or email my doctor about a prescription change, I don't think that the company is going to pick that up, and use it to market things.

PHAWKER: Hasn't the groundwork for that already been laid, with the way the NSA currently hoovers up all web traffic and keeps it in massive databases? If they want they could look at every e-mail you ever sent, every web search…

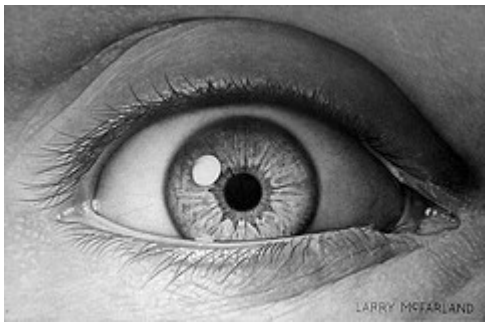
LORI ANDREWS: I do, in my book, talk about the 350 search terms that Homeland Security looks for in your e-mails — but that's different, in that they don't make it available to potential employers. They're not commercializing my data, which I find really problematic.

PHAWKER: Aren't we already pretty far down the slippery slope? Five years ago when all this was made public information, that the federal government had made arrangements with every major

carrier (AT&T, Verizon, etc.) to put taps on everything, and the American public just kind of shrugged.

LORI ANDREWS: I think we should totally fight for those rights in both areas, vis-à-vis government, and the commercial sector. For example, I do not think the cops should be able to get information from social networks without a warrant. That's another area where I think the rules should apply as they apply offline. It's the 225th anniversary of the U.S. Constitution, which is why I'm excited about launching the book in Philadelphia where the Constitution was drafted. I'm advocating a Constitution for social networks that is very much about applying those Constitutional rights we already have to a new setting.

PHAWKER: If social networking had been around when the Constitution was drafted, how do you think it would be different?



LORI ANDREWS: First of all, there are big parallels—I actually think you should have a right to connect, and be troubled by things like governments trying to come up with a "kill switch." I think that, very much, is akin to freedom of press. I think that you should have the kind of free speech on social networks to be able to say things that are critical of your boss or your job. But I think there would be some other rights, like a right to privacy of place, and so I think about the Pennsylvania case where they gave high school students laptops from the school, and then unbeknownst to the students or their parents, officials at the school would turn on the cameras, and take pictures of the kids in their bedrooms.

PHAWKER: Getting back to the "kill switch" that you mentioned, you're talking about the way the Egyptian government was able to shut down the Internet during the Arab Spring uprisings?

LORI ANDREWS: Yes. An equivalent approach in the U.S., was being considered prior to Egypt. In Egypt, they were able to do it by calling the handful of Internet service providers, and having them shut down. We've got thousands [of ISPs] in the U.S., but some of the things being considered are requiring digital tags to be put on transmissions, so you can indicate where they're from, and having Homeland Security be actually able to refuse to allow the transmission, actually turn off some with certain digital tags, so being able to turn off transmissions from a particular place, or from a particular set of individuals, and you can see how that would totally conflict with a primary Constitutional right to connect. It's funny, some countries are way better than the U.S. about this kind of thing, like Estonia has a right to connect that includes even having Internet access points within a certain distance of your home, and being able to access the Internet for free, if you can't otherwise.

PHAWKER: Where does that whole "kill switch" thing stand currently, in this country?

LORI ANDREWS: There's still legislation that's being talked about along those lines.

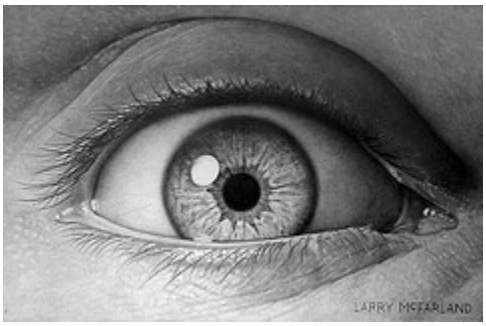
PHAWKER: So it's still in the talking stage?

LORI ANDREWS: There's been some bills introduced that would give Homeland Security that power, but they haven't been passed yet.

PHAWKER: Do you find it disturbing that so much American software technology is being exported to dictatorships and used to track down dissidents on Internet? People are being arrested, beaten, imprisoned or killed and it was this American software that made it all possible?

LORI ANDREWS: There is a call among some in Congress to look at the digital monitoring software exports the same way we look at weapons exports, and actually require companies to disclose who this is going to, and for what purposes. And it seems like some of the software used to punish those people for the uprising, to jail, and so forth, came from the U.S.

PHAWKER: A lot of the time it's sold to a third party, who then sells it to Syria, or then sells it to Iran or Egypt and the American company just shrugs and says they can't control what happens to their product after they sell it.



LORI ANDREWS: There are some people in Congress who have concerns about that, and are trying to do something about it. It's very much akin to selling weapons abroad, and putting restrictions on what the purchasing country can do, but you raised a good question about how effective that really is.

PHAWKER: Why are none of these things we area talking about being addressed by Congress? I'm asking this question rhetorically because I already know the answer: Because Facebook and other big data companies give massive amounts of money to congressional candidates and hire lobbyists to strong arm any that that can't buy. If campaigns were publicly financed, and corporate special interests couldn't give politicians any money, do you think a lot of these things you're talking about would actually have been addressed a while ago?

LORI ANDREWS: I think certainly it would make a difference to have publicly funded campaigns. I think also many people don't know this is going on. Until I started this book, I didn't know about data aggregators. I didn't know about sites likeSpokeo.com,, where you enter a person's name, and it'll tell you their estimated worth for a free subscription, and then for more money, they say they can give you any photos that are published on the web. So part of it is that we don't even realize that this is happening to us, and there are a couple people in Congress—Al Franken, Patrick Leahy—who are trying to do something, but often what they're trying to do is very narrow, like limiting law enforcement use. So we really need someone to come up with a more comprehensive approach to what's going on, and ways to handle it. That's why I thought "the Constitution," which people are really aware of. They know about the Miranda rights, and

so forth, and I think we should have a similar kind of warning system, that says, "you have the right to remain silent."

PHAWKER: Dictionary.com is one of the most aggressive, in terms of putting cookies on you, is that correct?

LORI ANDREWS: They put 233 cookies on your computer when you use their web site, according to The Wall Street Journal.

PHAWKER: Jesus! Is there a "silver bullet" solution to all this, or is it going to be incremental—one thing at a time?

LORI ANDREWS: I think we should change the default position—no data collection, unless we opt in—that would take care of a lot of this. And then maybe some laws about third parties, for example, employers can't Google an applicant, and then not hire them based on what they find there.

"Q&A: With Online Privacy Expert Lori Andrews," Jan. 12, 2012, http://www.phawker.com/2012/01/12/qa-with-online-privacy-expert-lori-andrews/.