SMU Science and Technology Law Review

Volume 14 | Number 3 Article 4

January 2011

Privacy: Problems and Solutions

Privacy: Problems and Solutions

Moderator:

Professor Xuan-Thao Nguyen, SMU Dedman School of Law

Panelists:

Jennifer Archie, Partner, Latham & Watkins LLP

Andrew S. Ehmke, Partner, Haynes and Boone, LLP

Dr. Joshua Fairfield, Washington & Lee School of Law

Berin Szoka, Founder, TechFreedom

PROFESSOR NGUYEN: Good afternoon, and thank you. I know from participating in this conference in the past that you, the audience, are the experts. And so we want a conversation with you on this topic, which you know so well. Before we go to the conference with respect to the panel on privacy, I want to recognize the hard work of one of my students, Jesse Adkins. He spent endless hours doing research to help prepare for this panel. Last year the feedback from the audience was overwhelmingly positive, so his work is greatly appreciated.

I am so pleased to have the panel that is here today. We have Jennifer Archie. She is a partner at the D.C. office of Latham & Watkins. She specializes in communication law, Internet, new media, and privacy law. Then we have Joshua Fairfield. He is an Associate Professor from Washington & Lee Law School in Washington, D.C. He writes and teaches in the areas of e-commerce, new media, and also privacy. We also have Berin Szoka from a privacy think tank group. He is the President and Founder of TechFreedom. He was in private practice for several years before he decided that he wanted to make "an honest living," and he decided to go and join a think tank group.

Then, we have Andy Ehmke. He is a partner at Haynes & Boone in the Dallas office. Andy is an IP and patent attorney. He is also a games attorney. He is an editor of the video game law blog called Lawyers in a Gamer's World.[1] So as you can see, we have these incredible panelists up here. But—as I stated before—you the audience are also the experts in this field. I would like to have an interactive panel discussion and at any time I would like you to engage in the discussion with us.

First of all, what we will do is I will pretend to be Kool Games Company, so instead of the KGB, I am the KGC. I am the Kool Games Company and have been legal opting games. I am biased and think my games are really cool. I am not one of those big puppet shows out there. I am not one of those big legal offers out there yet, not at this stage. But I think that, nonetheless, I have some really cool games and that my games are for both adults and children. At this particular stage, we are still tweaking, designing, and working on our games. At this stage then, are there some privacy concerns with which the panelists can help me?

---

1. Andy Ehmke, LAWYERS IN A GAMER'S WORLD, http://www.lawyersinagamersworld.com/.

By the way, since I am at Kool Games Company, and we are at this early phase, keep in mind that I do not have a Chief Privacy Officer in my company. I am the Jack of all trades—in fact, Jill of all trades—because I have to do everything that relates to legal at my company. I am overworked and underpaid. I want to get free advice from the panelists. Specifically, I want to know whether at this stage I should be concerned about any privacy issues at all. I will leave it up to the panelists to take turns and engage in this discussion.

MR. SZOKA: Well, let me just start by saying that this is not actually a panel just about law. Instead, this is really about brand management, public relations, and risk management. Everything we are talking about here today is not just about getting sued or having a user complains. It is also about the chance that you might show up in the *Wall Street Journal* and their series on privacy, or you might otherwise get some unwanted attention from your Attorney General. The number one reason that you should pay attention to this stuff is that it is not just about legal risk. It is about managing your brand and how people perceive you, which are both risks and opportunities. You have the opportunity to actually do good things and empower users and take privacy seriously in a way that does not cripple your business.

MR. EHMKE: And I would say—like all things legal—you are already coming to me too late.

PROFESSOR NGUYEN: Oh my gosh! I have come to you too late? Are you sure I am coming too late? Does anyone in the audience agree with that? Am I coming to him too late at this stage?

MR. EHMKE: Later than I would have preferred. If you are already finished with the game, then what you are doing is just tweaking. One of the aspects here is planning ahead and thinking about what you are going to try to do. You might want to consider thinking about what the privacy aspects of your game are going to be at the beginning stages. What information are you collecting? What information do you need that you are planning on monetizing with respect to the game? Because that might direct how you are building the game.

MS. ARCHIE: Yes, you are probably too late. I think that privacy in the last two or three years has really been front and center in Washington and among the states' Attorneys General when grasping how to harmonize what is going on with the E.U. and everywhere else. If you are already out there gathering up players and their data, a heck of a lot of stuff has already happened with regard to privacy. Because privacy really comes down to the following: What do you collect? Do people know what you collect? Who do you share it with? What choices do you give members? Is your data accurate? What do you combine it with? Are your players going to have control over the ability to delete an account? Or are they going to have granular controls, crude on/off switch-type controls, or no controls? What is the security of the data? These are all the core privacy principles that have been identified for decades now. If you have already built the game, then it is kind of too late. You have to be pretty smart about that and very deliberate. That

way you do not end up with an expensive fix later when you finally get to a lawyer's office and the lawyer says that you are clearly attracting and you have users, but now you have IP addresses that would have been so easy if you just figured out a way to just hash that and not actually collect the data. It is just important to have early attention at the product development phase.

MR. SZOKA: We are not going to talk much today about policy because we are trying to focus on core issues that you will face. The key term you will hear about in privacy discussions now is 'privacy by design,' which means not waiting until the last minute to sort of tack things on at the end. Instead—just exactly as Jennifer has been saying—you think about what you are doing ahead of time. Bake it into your game, into your system, and into everything that you are building. Decide how you think about privacy, what controls you are getting, transparency, and some accountability. But also think about those things as you build out your organization. We will talk about this a little bit, but privacy is not just about features. It is primarily about people and processes.

DR. FAIRFIELD: We have talked about the customers right there at the source of the privacy concerns. We have talked about D.C. as a source of potential privacy threat in terms of regulations. We have talked about the *Wall Street Journal* press as a source of some nervousness about what your privacy policy might be subjected to in the media. Another thing to keep in mind is with whom you are working. One thing that we are seeing is that increasing numbers of small game companies are looking wherever they can for money. And sometimes they are looking to government, not as a source of regulation, but as a source of grants.

There are a whole series of extra concerns when you get in bed with government or if you are spinning your company off from an academic setting—which happens a lot. Or, if you are entering a collaboration where you think: "Gee, wouldn't it be great if we just took all of this data that we have not hashed all the IP addresses from and handed it off to some academic researcher who is going to do magical, wonderful things to it and return to you all kinds of neat monetizable information about your customers." I will not go into the law of it here because there is nothing that will kill a cocktail party conversation faster than a deep law discussion.

Just remember that the people from the government who are thinking about whether you are holding up your end of the privacy deal are people who are used to looking at medical experiments, i.e. the Nuremberg Trials, the Tuskegee syphilis experiments. They are applying a lot of those rules to simple social science and computer science experiments. So again, who you are working with may also determine your risk tolerances. It does not have to be just the government. It could be anything. Are you working with angel-investment capital? What is their risk tolerance? Are you working with venture capital? What is their risk tolerance? What have they built in? The coalition that you have put together to form your group may well drive your risk tolerances and what is acceptable for you in terms of a privacy policy.

PROFESSOR NGUYEN: Has anyone in the audience done any work relating to or upon various agencies in the government whether state governments or federal governments? Or do you know of anyone who has done that type work? I think that the Guildhall's Professor Peter Raad obtained a $2.5 million project with one of the government agencies. Anyone in the audience? Yes, there is one. Do you want to share with us your experience in terms of privacy related to working on projects with the government in the games industry?

AUDIENCE QUESTION: We have had a variety of products with the DOD (Department of Defense) and with difference defense agencies with different security clearance levels, so the privacy that we have been working with has mostly been top-secret clearance and things like that.

PROFESSOR NGUYEN: Do you have in-house attorneys or outside lawyers working with you on that? Do you have a Chief Privacy Officer or somebody to handle that? Or do you take care of it?

AUDIENCE QUESTION: For most of it, we have in-house counsel who work with some outside counsel. Often it comes down to the prime contractors that we are working with that take on that lead position with the government.

PROFESSOR NGUYEN: Is there any takeaway that you want to share with the audience and our panel up here? Is there any lesson learned from that or anything that you think that relates to government funding and privacies here?

AUDIENCE QUESTION: I think the number one takeaway is that it is radically different than working in the private sector with traditional game publishers. Because at a basic level, the motivations behind the project are completely different, the business models are completely different, the accounting standards are different, and the purposes are different. It is just a radically different world. What we have found is that to be successful with projects like that, we needed to partner up with a group that is either a prime contractor or subcontractor with the government and specializes in those kinds of things. You cannot take it for granted that a traditional game developer will have all of the right shops to do the right thing.

PROFESSOR NGUYEN: Great, thank you. This is exactly what I want: the audience engaged in the discussions. Let's continue with that. Now, I know that the next panel discussion will focus on growth, and growth is key here. As my company is growing, the player base and the data I am collecting are growing as well. On the one hand, I am happy. But on the other hand, what would you—the panelists—advise me to specifically watch out for?

MR. SZOKA: We started to talk about this, and the key thing—the first thing—is privacy by design. In other words, thinking ahead of time about how you are using data, what controls you are building in, and so on. My colleagues will talk more about your terms of service and how you should get all of that stuff in order. The other thing that you really have to pay attention to is the internal infrastructure in your company that deals with this. Who is

actually thinking through and being responsible for how you are using data? The Google Street View example is the perfect case of how not to do this.[2] One engineer made a mistake by including a code that collected and saved packets that were being sent out on secured Wi-Fi networks and were in a tool that otherwise did not need to collect that data. This mistake was overlooked because there was not a sufficiently clear set of internal safeguards to make sure that everyone knew what data was being collected, that it was being used, and how it was being used. My answer is to construct an internal infrastructure that is responsible for privacy and thinks about it in the legal sense—but also in a brand- and PR-management sense—so that you are prepared when a reporter calls you and asks about your privacy practices. That way you can tell a good news story, as well as try to allay questions that maybe are not so flattering.

MS. ARCHIE: I think that someone also has to have that accountability and say: "It is my job that we think about this at the product development stage." What Berin is also saying is that it has to involve checks and balances, and maybe that is just one Jill-of-all-trades who has to do that. Someone really needs to—and I use this word in quotes because I do not mean it literally—"audit" in a thoughtful way. What is the data that is being collected? What is it that we are getting? That way there are no unnecessary and inadvertent data collected. You want the data that you need to make the game addicting in the best sense, fun, and monetizable. That is the data set that you want. Everyone can agree on that in theory, but how you get there at the product development stage is kind of slow and tedious. You have to have checks and balances at an engineering level. You will probably need a lawyer-like person that knows how to ask the checklist of questions.

The other thing I wanted to say about a company at this stage is that at the very beginning people think: "I just have to build it, and they need to come. I need players. I need eyeballs. That is what I need, clicks and eyeballs and engagement with my games." So they want to make that registration flow, lickety split. That is the goal, lickety split. That is the only thing. That is something else to really pause on because once you launch that registration flow, it is pretty hard to change it later on. It is really important. It is like thinking of your logo. What are the cool words? What is the vocabulary? What is the look and feel of the registration flow? What data is collected there, and how is it presented? It is really the first handshake with the members. It is very important in a game setting to have that be a binding contract. Because—in gaming above many other kinds of paths of things on the internet—there is a lot of IP on the line, and there are bad behaviors that you need to punish, deter, and block, and then you have to get those people off. Gaming companies need to be able to rely on those terms of service, and so the registration flow is something not to just throw up in any old form or

2. Jared Newman, *Google Street View Privacy Breach: Lawmakers Get Mad*, PCWORLD (May 20, 2010), http://www.pcworld.com/article/196770/google_street_view_privacy_breach_lawmakers_get_mad.html.

copy somebody else's. Do not say, "I do not care, all we need is the email and the credit card," which are the least the merchant banks will let you get away with.

MR. EHMKE: I would reiterate that one of the issues is, what are you collecting and why? A lot of times what I see is accidental collection or collection in a manner that is not expected, particularly as the company grows. You have different individuals and different competing interests within the company that want to do things. There is accidental collection. For example, the IP address and timestamp could be very valuable information internally just for tracking purposes, but also it can turn into something else when the marketing folks get their hands on it. Marketing can tie it to an account and know what that person is doing and when. There is a lot of collection that occurs, and the issue is first, detecting and realizing that you are collecting it, and then figuring out who within the company is actually using that information. Many times there is a realization of: "Oh my goodness, I did not know that someone was using that information to do X, Y, and Z, and I never expected or intended that."

MR. SZOKA: Let me just make concrete a point that Jennifer was making when she said "checks and balances." For example, we have people in the marketing department think: "Oh, this is great. We have this data, and we can do the following with it." I am pro-data. Unlike all the folks in the privacy community, I am all in favor of people making money in this field. But it is really important that someone in the company is there to sit on the other's shoulders and say: "Hold on a second. Let's think very carefully about how this is going to look and whether it is consistent with our terms of service. What have recent enforcement actions said about this?" Again, there has to be that kind of back and forth inside the company or it will come back to bite you.

DR. FAIRFIELD: I want to give you one concrete example of this that I think some people do not think about until it is late in the process. If you are collecting this data, there are people out there, such as law enforcement officials or people in the intelligence community, who are going to be interested in this data. If you get it big enough, they are going to come looking for it, so you need to have a policy in place. You need to figure out what your response is going to be if you get a § 2703(d) order requesting your customers' personal information.[3] You need to decide under what circumstances you are going to reveal information. Are you going to require there be an authorization order by a judge? Are you going to hold out for a warrant? How forward leaning do you want to be on this? This is a very concrete example of a way that you need to be ready to deal with the data that you collect.

Another thing I would like to point out is that we have been talking about data that you collect as the game creator. Remember, there is a whole other set of data out there that you need to manage—the data that your users

3. 18 U.S.C. § 2703(d) (West 2009).

collect on each other. You need to plan how you will manage how users are going to be using the data forms in—and often through—communities. Users are going to be busy executing each other, tossing people out, and trying to get you to ban them. They are going to be *doxing* each other, meaning they will be putting up all kinds of personal information about a person that they do not like as an online attack. You need to have responses in place for the data that you are not collecting, but that is still being funneled through your system because it is being used by your user base against your user base.

MR. SZOKA: Just to reiterate, these issues that we have been talking about, such as how you deal with privacy from a branding perspective and from a user management perspective, are also inseparable from other issues like how you deal with online child-safety protection to the extent that kids are going to be playing your games whether you say that they can or not. They are also inseparable from the issue of how you deal with policing speech and conduct on the site. These issues matter, because somebody out there somewhere is going to die related to a game. Some interaction is going to lead to something awful in the real world, and it is going to look really bad. It will also probably make you and your employees feel really bad if it actually happens. These are all reasons why it really does matter that you have a process in place for thinking about these things ahead of time and building them into how you design your system.

Whenever any one of us does this sort of talk, we always get the question: What is privacy? Is privacy totally amorphous? One resource I highly recommend is Professor Daniel Solove's book, *Understanding Privacy*.[4] Professor Solove has written some of the better books about defining privacy, and I urge you to read this one. He really does an excellent job of breaking down what the constituent's concerns might be. As just a simple concrete example of this, I have talked to people in the community who are developing new offerings, and they often say to me: "Well, this data is already available in one form, so all we are doing is giving it another way to be found." I think what Professor Solove's taxonomy does is give you a good sense of why someone might have an objection to that sort of approach based on privacy grounds. They might say: "Well, the data has become more accessible. I do not have to go to the DMV to get your driver's record now. I can pull it up online and then scrape everybody's driving records and put them into a database." That is just one example to give you a flavor of how this actually works.

I will say that in the privacy debate, there is a big philosophic-normative discussion about what the right questions are. In that respect, I disagree quite strongly with Professor Solove because I think there are tradeoffs in the real world about user experience, how you study data, and how you fund your sites and games—because this stuff does not happen for free. But the basic

4. DANIEL J. SOLOVE, UNDERSTANDING PRIVACY 101-70 (Harv. Univ. Press, 2008).

taxonomy, I think, is incredibly helpful. And it is just something that will help you—or whoever in your company is responsible for privacy policy—to spot issues, if you read it and think about it. You are thinking smartly about privacy because you are asking the right questions. I am happy to chat with anyone afterwards about that.

MS. ARCHIE: I think that, in terms of the data categories, a lot of the activity and the headlines this year have been about the difference between what is and is not personally identifiable information. We used to only collect a name, address, and phone number. And everyone kind of got their head around the California statutes, and what made something a data breach or not a data breach, and whether it was stored electronically and whether it had some security.[5] People developed this idea that if they were not collecting financial accounts and account passwords and other such personally identifiable stuff, they would collect it and just tell people that.

What we see now is that the data can now be combined, aggregated, automated, sold, transferred from one place to another, and all put together in one big pot. The browsers, the ISPs, and the ad networks all can collect the information, so the line between what is personally *identifiable* information and personally *identifying* information has gotten very blurred. For example, from all the headlines you would have thought that Facebook had suffered a data breach, such as a hack or something. But all that happened was that some of their apps could see user IDs.[6] If you were on your own Facebook page, your browser could say what your user ID was. In other words, is my user ID a piece of personally identifiable information now? There are a bunch of class-action lawsuits over this issue. Basically, whoever grabs the microphone gets to take a swipe at the brand. When you think in terms of: "What are we collecting?" it has gone way beyond what is on the form or on the first page.

MR. EHMKE: I want to ask a philosophical question. When we are thinking of video games, what are we defining as privacy? I know that when I play a game, I do not really think I have a whole lot of privacy, particularly when I am playing an online game. My expectation as the player is: "You know what? I think that developer is probably recording every key press and every mouse click I make." That is my expectation.

Now I am going to answer my own question. To me, privacy is the user's expectation of it. In other words, there is not a grand philosophical definition of privacy. I think there may be some disagreement on that piece, but when I think about the game context, privacy is all about the user's and the player's expectation. If you as the developer do not meet that expecta-

5. CA. BUS. & PROF. CODE § 22577a (West 2004).

6. Emily Steel and Geoffrey A. Fowler, *Facebook in Privacy Breach*, THE WALL STREET JOURNAL (Oct. 18, 2010), http://online.wsj.com/article/SB10001424052702304772804575558484075236968.html.

tion, regardless of what your policies say, then that is when you will run into a lot of problems.

MS. ARCHIE: There is such a power to shape that expectation. I think that is where Washington really has gotten us to say: "You know, they're completely away from the privacy policy." What is a privacy policy? A privacy policy is that big long thing you can link to and read at the bottom of the home page. It may or may not be referenced at the point of registration. At this point, if you are smart, privacy should be a common theme in your ongoing communications with your users. You should look for opportunities to teach and shape your user's privacy expectations. Users can have whatever passive expectations they have about privacy, and it will vary from person to person. But if you get into the litigation context, you need to have a set of materials that you can point to and say: "We use emails, we use pop-ups, we have a privacy center, and we have a million ways we push this information out. As a game developer we are not afraid to tell them what we know about them and find fun and friendly ways to do it." Put it in an email. There are so many push notifications in the world of gaming that there is no reason why you cannot clearly communicate privacy policies in a clever and attractive way.

DR. FAIRFIELD: These three themes—expectations, push notifications, and the expansion of privacy to cover user-identification numbers—are actually all the same issue. They are the same issue in the sense that, originally, most federal privacy legislation that governs an area of law such as human-subjects research defines personal information simply as anything that can be used to contact a real person in real life. At first such information was limited to name, phone number, address, and email address. But as soon as we extended it to email address, it was then extended to Twitter handles, and then to Facebook profiles, and then unique user-identification numbers.

The root of all of this is that our natural and important desire to communicate with our customers means that we are generating unique identifiers that permit someone to contact a real person in real life. By definition, those unique identifiers are pretty much personally identifiable private information. That is one of the reasons why you have got to watch this because it is an absolutely critical part of your business model. You cannot simply stop generating unique identifiers, but you need to understand that they are not just a series of digits anymore. Your Twitter handle is a legitimate way to communicate with a real person. If you send me an app message to Josh Fairfield, I will receive it. It is a way of contacting a real human being in the real world, and that means that for the purposes of these regulations, it is going to be treated as personal information.

MR. SZOKA: For my part, I think my friend Jim Harper at The Cato Institute is exactly right when he says the expectations test is a useful test when we are talking about government intrusion into our lives.[7] In general,

7. *See* Jim Harper, *Understanding Privacy—and the Real Threats to It*, 520 POL'Y ANALYSIS 1, 2 (Aug. 4, 2004), http://www.cato.org/pub_display.php?pub_id=

privacy is something really different. It is the subjective condition that we experience when we have the power to control information about ourselves. In short hand, privacy is empowerment. On a high level, if you were asking me: "What is the right thing to do?" in terms of A) corporate social responsibility or B) building a good brand, the right thing to do is protect your users' privacy against government to the limited extent that you can. You also want to empower users to the extent that you can by providing clear notices and useful tools to manage information about themselves in the game. That applies not just to the information that they share with you and how you use that information, but also to how they share that information with other users.

DR. FAIRFIELD: The empowerment—rather than the expectation—model not only has a big government versus private enterprise component, but it also has a generational component. Social research shows that Millennials—the generations that are coming online and using a lot of the games and social networks that we are building—actually have the empowerment view of privacy. They are all used to having their personal details out on Facebook. They are really mad when someone forwards something that they were not supposed to, i.e. when information gets out of their control. I think your user expectations may be evolving in the direction of this empowerment paradigm. And empowerment and expectation are actually the same thing in a lot of ways.

MR. SZOKA: Let me give you a concrete example, because I want to make sure this is clear. When I think about future privacy, I think about identity management. For example, right now Facebook offers lists so you can group people into lists of your friends.[8] You can share a particular post, status update, or an album only with that list. That is the kind of empowerment that I would like to see across the industry. Just imagine the end game. Imagine you have lists that you could synchronize across multiple games on the same platform, or maybe even tie to your Facebook friends list. This would allow you to have separate lists of your drinking buddies versus your work friends. And on your game, you can decide that you are only going to share certain information about yourself with that particular list of people. Such control is a form of empowerment because it allows people to show a different side of themselves to a different group of people and to do so easily.

AUDIENCE QUESTION: It seems like this is really wrapped up with a global concept of scraping. It seems to me that unless you can meaningfully take your data—your wall or whatever it is—and move it elsewhere to someone who is respecting your privacy policy in the event that the first guy does not, you do not have as meaningful of a remedy. In other words, you do not have a private-market remedy if you cannot take your data elsewhere. We may trust the government to impose sanctions or something, but until we can

---

1652 (discussing the government threat to the personal, subjective condition that is privacy).

8. Friends and List Privacy, *Facebook Help Center*, http://www.facebook.com/help/?page=768 (last visited Sept. 3, 2011).

move to that sort of mobility model, we are really lacking empowerment. Can you speak to that?

DR. SZOKA: Yes. To be precise, what you are talking about is data portability. Scraping is a different concern in which somebody else can just pull something off the site. In principle, what you are talking about is the most radical—and in some ways the most important—form of empowerment, which is the right of exit. It's the consumer saying: "I want to take my data with me and move it to some other game or platform." That is very much what I am talking about.

Let me also mention another spin on that, which is where we are going—and Josh will talk a little more about why that does not happen today. There is another dimension here. In the next generation of privacy, I would like to see not just the ability to move data, but also the ability to have interoperability of privacy controls across sites. Imagine if you could have the same lists and the same list structure in your game as on Facebook or on Picasa Web Albums.[9] That is another form of interoperability that is in many ways analogous to data portability, but they are both forms of empowerment.

MS. ARCHIE: Like eWallet, but for your identity?[10]

DR. FAIRFIELD: Unfortunately, there are no clear economic incentives for exit. In fact, lock-in is a business model. If you look at the public federal filings of a well-known game company, whose name I will not mention, they will say: "Hey, investors can have confidence in our company, because we will continue to do well. Why? Because our users would have to leave their entire social networks and all of their virtual property in order to leave our service. In other words, we have sufficiently constrained exit." Remember when we talk about exit as a great thing, and I think it is, and we talk about portability as a great thing, and I think it is, there are strong economic incentives that cut against letting people exit. These incentives are why, in user license agreements for most web 2.0 sites, you are going to see the opposite of an exit clause. You are going to see a clause that says: "If you leave, we may continue to use the data that you have posted." Such clauses are more common. There have been some famous defectors from the anti-exit clauses. MySpace defected after they had a user revolt finally saying: "All right, fine, if you exit, we will delete your stuff," but that is a more recent development, and it is not something that the economic incentives have naturally generated.[11]

9. *Id.*; *Picasa and Picasa Web Albums Help*, http://picasa.google.com/support/bin/answer.py?hl=en&answer=93973 (last visited Sept. 3, 2011).

10. eWallet, http://www.iliumsoft.com/ewallet (last visited Sept. 3, 2011).

11. Privacy Policy, (Feb. 28, 2008), http://www.myspace.com/index.cfm?fuseaction=misc.privacy.

AUDIENCE QUESTION: But to reverse that? It is data scraping, right? What if companies could start up like Power Ventures?[12] What if in fact they could scrape data to facilitate the portability by users?

DR. FAIRFIELD: They are going to get smacked with cyber-trespass suits. Yes, it is not great.

AUDIENCE QUESTION: That may be a solution.

MR. SZOKA: By the way, the specific case that Josh just mentioned is exactly why you have to have privacy people involved in your conversations.[13] Putting a line like that in your security filing is exactly the sort of thing that I, as a *Wall Street Journal* reporter, would be sure to use against you when I write an exposé about how terrible your privacy practices are. You really have to have integration between privacy, PR, and your legal people. Just to be clear, I do want to make sure I do justice to your question because what I think you were really getting at when you said scraping was one form that data portability can take today when it is not supported by a site.

DR. FAIRFIELD: The other site. . .

MR. SZOKA: . . . can scrape the data.

DR. FAIRFIELD: . . . will get it, and that of course causes cyber-trespass concerns.

AUDIENCE QUESTION: I just had a quick question that is going to illustrate my lack of knowledge and my non-lawyerliness about privacy. Specifically, my question is about behavior as distinguished from identity. I presume you are all familiar with *Valve* and *Steam* as services, just to use an example.[14] What if the identity of the user is unknown but the user's behavior is known? Let's say there is a lobby that has advertising in it, and I am not identifying who the user is or any information about identity, but I know what their behavior is. I know what games they play. I know how much money they spend. I know how long they spend online, and what they do in those games. I know with whom they play, and some characteristics about those things. What if I go and sell that data? For example, I use it to market or find advertisers for those particular people. Is there a privacy issue around my selling their behavior as distinguished explicitly from their identity, or what you would consider conventionally personally identifiable information, name, address, et cetera?

---

12. Facebook, Inc. v. Power Ventures, Inc., No. C 08-5780 JF(RS), 2009 WL 1299698, at *2 (N.D. Cal. May 11, 2009).

13. Privacy Policy, (Feb. 28, 2008), http://www.myspace.com/index.cfm?fuseaction=misc.privacy.

14. *Steam, The Ultimate Online Game Platform*, STEAM, http://store.steampowered.com/about/http://legacy.gateway.kctcs.edu/BIS/valuestreammapping.htmlhttp://legacy.gateway.kctcs.edu/BIS/valuestreammapping.html (last visited Sept. 3, 2011).

DR. FAIRFIELD: I think that is one thing we all do. People buy and sell click-stream data. People buy and sell game-performance data. If it is adequately hashed, you have really limited your exposure to a privacy claim. The difficulty is that as we get better and better at drilling down on behavior, at some point, you paint a picture of the person.

MS. ARCHIE: This becomes an issue, especially with the geography that is associated with the behavior.

DR. FAIRFIELD: With geo-location devices all bets are off, because with such devices you know not just their behavior but also where they are within about three-meter accuracy, all the time. That is a perfect example of the drill-down because at a certain point, your behavioral picture becomes the person and that becomes personally identifiable information.

MS. ARCHIE: For their legal rights, they have to be the legal rights of an identifiable person. In other words, the information has to be connected to a real-live human being. It is pretty easy and very common to boil that down to the point where you do not inadvertently connect the identifiable information. For example, consider search results or anything that has a search engine in which users contribute their own data. Recently, the FTC had an enforcement action related to a kid's web-surfing parental-protection product.[15] The big problem in the action dealt with all this user-entered data and the collection of so much information. People will reveal amazing things. This is slightly off-topic because it is not games-specific, but people really reveal a lot about themselves not only on games, but also on websites like health or parenting websites. It is unbelievable when you consider the identifiable information that users are contributing and that it is pretty easy to have that information get swept up in what someone thinks they can monetize, package, and describe.

MR. SZOKA: I think that one practical takeaway here is that as you think about evolving consumer expectations, you also need to think about the fact that business practices are evolving over time. They are evolving because companies are, in many ways, doing the right thing more often and more seriously, because government is bringing enforcement actions, and because the technology is changing. If you are trying to decide what to do with user data and how to use it, keep in mind that part of what we were talking about when we discussed internal processes and privacy by design is being up to what the state of the art is on keeping that data anonymous. You do not need to reinvent the wheel. You should be looking at what other people are doing in the business. You should do so because it will protect you from legal liability. Also, it is a story you can tell to the media. And generally speaking, it is the right thing to do.

PROFESSOR NGUYEN: Zach has opened up the subject of monetization. Flowing from that, if I share identifiable data or behavior-related data

15. Press Release, Fed. Trade Comm'n, Mobile Apps Developer Settles FTC Charges It Violated Children's Privacy Rule (Aug. 15, 2011), *available at* http://www.ftc.gov/opa/2011/08/w3mobileapps.shtm.

with partners, what are some of the privacy issues? This is just sharing for monetization purposes.

MR. EHMKE: To me, the moment you send the information outside your company, it becomes a "completely different issue." I used air quotes on this because it is still fundamentally a privacy issue. I would go back to my buzzword: expectation. What have you conveyed? What have you told your customers about your willingness to share their information? Did you put it in a single sentence buried at the end of a privacy policy fourteen pages deep, or is it part of something in bold font that they clicked on and agreed to? What is it that you told them you were going to do, and how explicit were you in doing it? Did you say: "I am going to share demographic information that has been aggregated," or "I am going to share your information"—which has different aspects on the monetization side.

MS. ARCHIE: There is a tremendous vernacular for that paragraph in a standard privacy policy, which is the long, big document linked to from the home page. People all go read each other's privacy policies. They block and copy these documents, especially during the start-up phase. Such actions are largely aspiration. They think: "I would like to be like that, so we will copy them."

MR. SZOKA: Sometimes people forget to do the find and replace.

MS. ARCHIE: Yes, you are right and that does happen. I think such copying is often very mealy-mouthed. People are trying to reserve every possible sale and transfer option they can without spooking anybody. Often, lawyers are asked specific questions, such as: "Can we sell this? It is a joint venture. It is just a pure data transfer. It is a we-are-going-out-of-business sale." The privacy policy can reflect any kind of context, but the words really often miss. Even if you communicate them in some acceptable fashion, they often miss. It is really one of the most devilish things to draft a privacy policy. Because the law and the legal perspective disfavor just staking a claim to territory by saying: "I might sell it to Santa Claus. I might do this. I might do anything I can think of, and this is not a complete list of the things I might do." Such privacy policies are not going to get you anywhere when you get down to a specific transaction within all that carved-out territory. It is a common practice, and everyone does it, but the FTC is unimpressed and unwilling to enforce such broad privacy policies.

MR. SZOKA: Journalists are even less amused. If you want to do something that is both good and proactive, then that will cause you to think this through carefully, I would encourage you to look at what companies like Google—who has done this best—or Yahoo, or Facebook have done. On the Google privacy channel, Google has a series of videos that explain in lay terms what Google does with all the data, including how it works and how it is used on the site.[16] I think this is great because it causes them to have to think through more clearly what Jennifer has been saying. Instead of throw-

16. *The Google Privacy Channel*, YOUTUBE.COM (Jan. 26, 2010), http://www.youtube.com/user/googleprivacy.

ing everything in, they have considered how to boil it down for the layperson. Such efforts also produce a clear, intelligible product to which you can direct users or journalists. Additionally, when you talk to people in the privacy community, you can point them to that. If something should ever happen with the media or a policy maker or law enforcement, you have something simple to point to and you can say: "We are not just hiding behind some wall of paper. We have really made an effort to go beyond and take extra steps to make this clear to users." The clear, intelligible product can be videos or FAQs. I encourage you to do not just the bare minimum and to think about these things carefully.

MS. ARCHIE: I always challenge my clients to think: "Let's focus on the unexpected." Do not say the obvious such as: "We are Amazon. We will use your information to ship product." Of course, you can put it in there if you want to have a complete list, but challenge the conversation to focus on the unexpected. Who is going to see it that you might not think about? How is it combined with other things? How are we monetizing this behind the scenes in ways you might not think about? That is the stuff that you need to find a way to pop up, put in a privacy center, and just embrace it. This is not 1998 anymore. That is part of what I want to say to people. There is an empowerment mentality, and it is ok to mention that you monetize your site, and you should be fairly clear about it.

PROFESSOR NGUYEN: Does this mean that if—in my privacy statement—I specifically state that I will share behavior data—but not identifiable data—with third parties, and I do in fact share this data behind closed doors, I am violating something? Under full disclosure, I am doing exactly what I promised, and I pointed out to everyone who came to my KGC website what I was going to do. Is there anything wrong in that scenario?

DR. FAIRFIELD: You can resell data. That is the American business model. The Europeans have a different model. If you have European users, you need to make a phone call. There are some people in this room who can help you with European-user issues.

Under the U.S. model, you can sell data as long as you have full disclosure. What we have been talking about are mistakes of disclosure. You would be surprised by how commonly they happen. I know this is shocking, but for one thing, your lawyer does not want to charge you more than he has to—which means that he is going to find what other people have said in privacy policies. He does this for two reasons: first, to save time on your billables, and second, certain language has been tested over and over again by courts, and it is safe language. By finding what other people have said in privacy policies, your lawyer is not just plagiarizing.

The problem with that straight rip-off is that if you do not read it with fresh eyes, you can end up with some real incongruities in your policies, and journalists love those. For example, some people will say on their front page: "We will absolutely never share your personal information," and then in their privacy policy they have a list at least thirteen sections long of all the people with whom the company will share your data. Someone designed the

front page. Someone else designed the privacy policy. But no one read the thing as a whole. Which goes back to our first starting principle: if you are the only person in the company, you need to be the person thinking about it. If there is someone else in the company as you grow, someone needs to be thinking about it, and he or she needs to be looking at these documents with fresh eyes and asking: "Does this fit my business model? Even if we have used tried, tested, and true language, does this really resonate with what we are doing?" If the policy language does not describe what you are doing, it is more dangerous to use traditional language for the sake of using traditional language than it is to just simply and honestly say what it is you are doing.

MS. ARCHIE: Maybe not because it is okay to change the privacy policy. That is something else we should discuss.

DR. FAIRFIELD: Oh, absolutely right.

MS. ARCHIE: Privacy policies have become more fluid. Five years ago companies tended to think: "We cannot amend our privacy policy. You will make us notify everybody. It will be a material change." But—more and more now—I see companies just declaring: "We have made a material change, and we posted it." Changing privacy policies has been sort of detoxed. I think it is okay to say: "Looking ahead two quarters, we could be looking at a transaction like this, and we need to take a deep breath, read the privacy policy, and try to fix the language to reflect our current business expectations."

DR. FAIRFIELD: But there are two real practical points there. First, you should build your policy at the outset to be able to change it. You need to say, "We are going to be able to change it . . ."

MS. ARCHIE: . . . and here is how we will tell you . . .

DR. FAIRFIELD: . . .and here is how we will tell you," and that is the second practical point. You cannot just say: "We can change it whenever we want, and you can just suck it up." Such an approach does not go over well with courts. You have to add a notification requirement. Some of the more brilliant ones I have seen simply said: "You give us an email address, and we will email you when we make a change." EFF, I think, has a great one where they just watch privacy policies, and when they change, they notify people.[17] If you just tell people about that, then they have a good scrolling list, or RSS feed, that simply updates whenever your privacy policy updates, so there is no way they can claim they did not get the notifications. To do something like that and to set up a notification regime means that you are going to have a fairly smooth transition if you make a mid-course correction.

MR. SZOKA: A lot of this is very similar to the advice that you might give someone to live a conscious life. A friend of mine has on his wall three

17. *See Privacy*, ELECTRONIC FRONTIER FOUNDATION, http://www.eff.org/issues/privacy (last visited Aug. 25, 2011).

takeaway points from David Allen's book *Getting Things Done.*[18] The three points are: What are you doing right now? What is your goal right now? Only one thing at a time.[19] In a sense, it is about a certain sort of Zen. It is about actually thinking through what you are doing and not just going through life on autopilot as we are want to do.

Such advice is essentially what we are suggesting here. Keep thinking on a day-to-day basis about what you are doing. Revise as necessary. Pay attention to evolving user expectations, evolving technologies, as well as best practices and enforcement actions. If you do all those things, and if you really practice this consciously inside your organization, you will probably be all right. If you think that you can just have somebody draft terms of service or just copy them from somebody else and then go along your merry way, you will eventually have a problem. And it could be a brand-killer, as Jennifer has said.

MS. ARCHIE: I think that in the bigger companies, you hear talk about how privacy has to be a C-level office because the studios have all the power. The studios generate the money and development, and their path often follows the idea that studios develop product, and they can just tell legal at the end. Then legal has to say: "Well, you have really tied my hands. I cannot have all these money issues." Thus, studios start thinking that lawyers are doing what they always do, which is delay launch by six weeks to discuss stupid issues that nobody cares about in the real world.

The companies that do it right have a sensitivity trained into the studio so that the developers and innovators in the company get why this needs to be thought about at the beginning. Then legal is not just "delay and obstruction," which is the usual rap the profession takes.

PROFESSOR NGUYEN: How about this scenario? Someone this morning—I think it was Joseph—talked about film financing and how the game industry has been looking at film financing as a model for financing in this industry.[20] Let's say that I, as KGC, did some work with people in film financing. And one of the kinds of financing relating to the finance of this industry is that the financier will provide the funding and take some equity. The financier also provides funds in exchange for a security interest in all of the assets present and to be generated, which usually means the intellectual property. In this case, the assets would also include consumer data and all the information relating to the consumers. The day that I, KGC, got the funding, the financier decided to take a security interest in all my assets.

18. David Allen, GETTING THINGS DONE: THE ART OF STRESS-FREE PRODUCTIVITY 13 (Penguin Books, 2003).

19. *Id.*

20. *See* Joseph Olin, President Emeritus, Academy of Interactive Arts and Science, Keynote Panel at the Southern Methodist University Science & Technology Law Review Game::Business::Law Symposium: The Law and Business of Video Games (Jan. 26, 2011).

Because KGC is a games company, all the assets are intangible assets. The contract I signed for KGC says: "I hereby grant a security interest in all of KGC assets, general and tangible," and so forth. The financing company will perfect the security interest, and they will file the financing statement.

What if KGC gets into financial trouble? One of the remedies available to the financing companies is that they can foreclose on the assets of the company. What if the financier in this case decides to foreclose on the assets, which means they can take all KGC's IP and consumer data as well? On my privacy statement, I stated that KGC would not share consumer data with any third party and would not sell data to any third party. In this scenario, KGC has not sold the consumer data. KGC has merely used the data as security, or collateral, to get financing. Is KGC violating the privacy statement? Is KGC in violation of any law? Or is this just part of the growth and pain itself? What do you guys think?

MR. EHMKE: I think this ties into Jennifer's point earlier that when you think about the privacy policy, you are not going to think of every situation. There are just too many different business events that are going to happen. Think about the scenario you just outlined. One, I need to get financing or I need to get a loan. And two, part of that financing was that all of my assets were going to be collateral. At the time of the agreement, I did not have the list of information. It was going to be developed eventually, so it became collateral. Then my business failed, and they foreclosed. When a foreclosure occurs, the bank will foreclose, and then sell the assets. Generally, a bank is not going to hold on to the assets. This means that during the financing process, the bank might say: "If you are going to use that information as collateral, I need to be able to sell it, but your current policy does not let me." In such a case, the policy becomes an impediment to getting collateral in the first place.

MS. ARCHIE: Such issues should come up in the diligence of whoever is doing those documents, and that person should ask: "Did we just grant ourselves a right we could never exercise?" I also think that *third party* is a really useless term because it is flexible. People think they can just say *third party*, but it has no meaning. I have litigated cases in which I tried to tell a judge the meaning of *third party* in a way that I can get a foothold somewhere and not just be drifting all over.

"What is a third party in this context?" You can always define family, so you can say: "Our investors are going to be family." That way you may be able to share with corporate affiliates. You may do business combinations. I mean there are certain basic and fundamental building blocks for which you do not have to cast a huge projection into some future that you do not really expect to happen. You can define your corporate family, investors, and others in that group in a way that gives you better language than *third party*. I cringe every time someone writes: "We do not sell or rent your name to third parties." Someone wrote that sentence in 1994, and it got copied everywhere.

MR. EHMKE: Shame on you for saying that you are never going to sell it, because you are. You absolutely are. You have an exit strategy. You want to be bought. You want someone to invest. You want to sell it off. You want to sell it. And to say that you are not simply means that you are not looking forward.

MS. ARCHIE: You might win on the definition of *third party*, but it is a roll of the dice. Because I am a litigator, I think about the business risks in terms of how do you want to set this up, so that your brand will never be in the *Wall Street Journal*? That is one level of conservatism and prudence. Alternatively, do you want to win it at a motion to dismiss? This approach means I just put my registration flow in, attach my terms, and attach all the little extra things so that I can prove to these named plaintiffs—or whomever tells the FTC that registrants were exposed—I win on motion to dismiss, and I think that I had insurance coverage for it. This is how policies typically get defended—an industry group gets sued, and it usually consists of several types of players. They all share counsel. So they think: "I will survive a motion to dismiss. I do not care, because I am a great big happy company now." Alternatively, they think: "Am I going to have to gut it out through discovery?" That is really painful and the reason why litigation is expensive. Such a strategy is a summary-judgment strategy. Relying on loosey-goosey language like *third party* is probably a trial strategy, but everyone knows that it is not a good strategy. It is a roll of the dice because you are going to let a jury or a judge that you do not know—in a forum you cannot yet imagine—decide whether you have a big legal problem or not. A lot of money gets tied up in these kinds of cases.

DR. FAIRFIELD: On the securitization point, I wish I could stand up and change places with Roxanne, who does this and has forgotten more of this than I will ever know. Securitization is a big issue when you talk about the set of circumstances that has to happen. The circumstances may sound implausible, but think about it. All financing statements have these broad, sweeping clauses that bring in all this collateral. So anytime you seek bank financing there will be such a clause in there, and you will have to deal with it sweeping in your IP. All financing statements are going to have a future-interest clause, which means that they are going to sweep all of the future IP that you generate. Unfortunately, a lot of video game companies fail. This means that you need to have an exit strategy that looks in that direction. Already, we have seen the first of these foreclosures. For example, Flagship Studios Hellgate: London had a film-financing model.[21] They went to the bank, and the bank took a security interest in the property.[22] The foreclosure did cause a bit of a train wreck between the overseas distributors who very much wanted to buy the entire property and the bank who was sitting on it saying: "No, we actually want to sell this. We are going to try to sell it at a

21. *See* Jeff Green, *Bill Roper Speaks Out At Last*, 1UP.COM, (Oct. 14, 2000), http://www.1up.com/features/bill-roper-speaks (last visited Oct. 2, 2011).

22. Green, *supra* note 21.

fire sale."[23] It really can tangle things up at the end of your company if you do not have the clear and clean ability to sell interests that have been subject to what is essentially a mortgage.

MR. SZOKA: I would like to make one other point. The government is not sitting idly by while all this is happening. I think it was last year that the Federal Trade Commission intervened in a bankruptcy proceeding for a magazine that was geared toward gay teens in order to prevent the sale of their user data.[24] Basically, the FTC just said: "No, we are going to take that asset off the table, and it cannot be sold in bankruptcy."

DR. FAIRFIELD: There are a couple of other cases like that, too.

MR. SZOKA: It is a pattern of which you should be aware.

PROFESSOR NGUYEN: Let me spin my problem a little bit. What if I am not in bankruptcy? What if I am not in foreclosure? Say I sign the security agreement that states: "I, as KGC, hereby grant a security interest in all of my assets to the financier." At that moment, am I in violation of any privacy law?

MS. ARCHIE: You have probably breached a representation or a warranty saying that you had the authority to transfer what you transferred. In the real world, I think that stuff gets worked out by somebody taking a look at the privacy policy and saying: "Eh, it does not breach." You could probably get somebody to give you some advice, unless there is a clear prohibition or complete silence. If there is a complete silence about transfers, or if you have a broad sweeping statement such as, "we never will," then you are in trouble.

PROFESSOR NGUYEN: Would it change your advice, if I had an exit strategy in terms of changing my policy statement to accommodate?

MS. ARCHIE: Then we get into the problem of retroactivity—whether you have to re-permission the entire database, and whether you can then only transfer those who gave their consent. This is a problem that happens in the real world. I think a lot of times, people just do a drive-by and say: "I will deal with it if it does not work, but that data is going to get transferred." I think nobody is going to receive legal advice that such a drive-by is the right thing to do.

MR. EHMKE: I have been a part of deals where the deal did not close because of such issues. They were selling themselves. They were going to make a lot of money, but the deal did not close when they wanted it to because the privacy policy said that they could not do what they wanted to do, and the company needed to follow the privacy policy in terms of notifying and letting people know that they were going to transfer consumer information.

---

23. Green, *supra* note 21.

24. Letter from David C. Vladeck, Dir. of the Bureau of Consumer Prot., to Peter Larson and Martin E. Shmagin (July 1, 2010), *available at* http://www.ftc.gov/os/closings/100712xy.pdf.

MS. ARCHIE: It is a reasonable strategy if you write a really reasonable and robust notice that says: "We will notify you, and you will have a period of thirty days within which you may opt out. After that we deem that you have consented." It is a lot more fun to do that when you have warned them. I think Josh exactly described what the provision would be.

MR. EHMKE: Also, you become very unhappy when that check with a lot of zeros is going to be delayed thirty days. You were about the pop the champagne, and now you have to wait thirty days because of your privacy policy.

PROFESSOR NGUYEN: Any questions from the audience?

QUESTION: On the issue of thirty-day notice, how many private companies are really instituting that? I would be hard-pressed to convince a client that they need to announce to their user base that they are about to get acquired. It seems like that approach is going to be pretty problematic. In fact, a lot of the privacy policies that I see state: "We would be able to sell or transfer that information upon an acquisition, and we will provide notice of the transfer." Do you find that to be a defective notice?

MS. ARCHIE: From an FTC standpoint, a problem arises where there have been express assurances. Whether your name will be sold in the event of a business combination or transfer is a material fact. You can write it down on a tablet that the FTC has said that whether your information will be transferred on is a material fact. Can you notify and tell people when a material change is happening in your privacy policy and then impose it retroactively? You can do what you warned them and told them in advance you would do. Often, there are very awkward situations involving legacy users and how you deal with them. The notice is how you deal with them. No one is saying you are going to leak non-public information to your users first, but it gets factored into the timeline of how a deal closes.

MR. EHMKE: One particular scenario that was very tangled involved an existing policy of an existing user base and did not provide a clean mechanism for subsequent transfer of the assets. The existing rule set—the policy is now the contract with your customer base—did not contemplate the transaction that was going to happen. You then at that moment say: "Am I going to cut off that asset and not transfer it, or is that an important asset that needs to go?" Now, what am I going to do to correct the situation? Am I going to modify the privacy policy? If I am going to modify the policy, does the policy give instructions on how to do so? Does the modification apply retroactively to that client base? In my opinion, this is the thorniest issue.

What if your existing policy says the user is going to agree to the new policy, notice will be provided, and the next time the user comes to the site represents an agreement to the policy? What about the thousands of users that have not gone to your site since the change, but now you are ready to do the transaction?

MS. ARCHIE: The Federal Trade Commission is all over these hypotheticals. It is a top five in privacy policies.

DR. FAIRFIELD: This just happened when Linden Labs did a huge revision in the *Second Life* terms of use.[25] People were up in arms about it, because Linden Labs included a requirement that users cannot use the site until they log in and accept the new terms of service. There was a lot of buzz going around that they were especially making those changes with respect to who owns the intellectual property within the virtual world. There was a lot of speculation the change was made in order to facilitate an acquisition. Sometimes you cannot avoid making a change because you decide you cannot sell it the way it is now. You have to make a change. And you have to provide notice, which is unpleasant. But there is no way around it.

MR. SZOKA: I think people already know this, but it might be helpful just to repeat what we talked about with these practices, these terms of services, and so on. The underlying law that actually is at work here is the Federal Trade Commission's authority to punish both unfair and deceptive trade practices. It is not just that you do or don't do what you say you are going to do. For example, there are certain circumstances in which an omission—which Jennifer was talking about earlier—could be potentially actionable. We do not need to unpack that completely, but on a high level I think it is important to understand that this is the essential or primary backdrop of U.S. privacy law. There are also what are called sectoral laws that apply to specific issues, like kids, for example.

PROFESSOR NGUYEN: Are there any other questions from the audience relating to financing, partnering, licensing, or anything similar that you want to provide comments, questions, or your answers to some of these problems?

MR. EHMKE: I have a question for folks out there. As app stores are starting to become more prevalent and games are being distributed, are people thinking or doing anything about the issue of contract privity? There is a distribution mechanism happening through the Android marketplace or the Apple App Store, and both are collecting certain sets of information. And your game will also be collecting information to relay back to you, which creates a weird three-party triangle of information collection.

MS. ARCHIE: And a great big list of others.

MR. EHMKE: The triangle consists of many different nodes.

MR. SZOKA: I just want to point out that this has been a huge issue in media. For example, I hate to pick on the *Wall Street Journal* but they have had good coverage on how this issue has played out on Facebook.[26] Jennifer already mentioned one of these cases earlier for which the question is: what data is being shared with app developers? Is Facebook transmitting all the information they mean to be transmitting, or are there inadvertent transmissions of user IDs? The same issue is true on multiple platforms, like on

25. Linden Labs, *Terms of Service* (Dec. 15, 2010), http://secondlife.com/corporate/tos.php.

26. Steel, *supra* note 6.

Android. This is an area where law, technology, user expectations, and best practices—the four areas we talked about earlier—will continue to evolve dramatically.

How exactly do you manage notifying users about what information is being collected by the game provided in the Android marketplace? To some extent this is governed by essentially private law—an example of which is Google's terms of service for its own marketplace.[27] While we could have a whole panel just on that, it is sufficient to point out that it is a hugely important issue that should be at the top of your list if you are working in this area.

MS. ARCHIE: It is not an overstatement to say that notice and choice are not really functional on that type of platform, as opposed to a PC or Mac full-screen environment or even a console environment, which allow you to collect more consent. In a marketplace environment, if you click "install," then you agree to those terms. The only thing they really are good at telling you is that they might push marketing out to you.

MR. SZOKA: On a high level, Jennifer, I think what you are getting at is that because it is more difficult to give notice to what you are doing, there becomes more pressure placed on you to exercise good stewardship of data and also to follow fair information practices more closely. For example, if you are making a game available, it is probably not a good idea to say the game taps into the user's phone contact book if that is not necessary. That example is the kind of thing that, whether by law or by pressure from the platform operator or from the media, is going to evolve certainly as an industry best practice if not as a regulatory mandate, which again might well happen.

MS. ARCHIE: I think this is where the taxonomy approach is relevant. What are we doing that is really spooky? I always think of the collection of data as unexpected, but there are other ways of doing it. The question is, what are the tripwires on privacy? And how do they apply to my unique, cool, fun way to interact with others? If you don't ask the question at the outset, then you cannot begin to deal with the fallout later.

PROFESSOR NGUYEN: Professor Raad has a question. Let me hear from the audience.

PROFESSOR RAAD: I want to pick up on the word "choice" that you used. The picture of my pool in the front of my house is on Google. I never acquiesced to that. I guess in Germany hundreds of thousands of people are up in arms that Google would block out their home.[28] When you say "choice," what is my choice? Is it to continue to play the game, or to read the 73,917 pages of legal stuff that I really do not understand? I have gotten to the point as a consumer that I just push okay. I cannot read this stuff

27. *The Google Privacy Channel*, *supra* note 16.

28. Mickmel, *Street View Finally Launches in Germany*, GOOGLE EARTH BLOG (Nov. 2, 2010, 8:07 AM), http://www.gearthblog.com/blog/archives/2010/11/street_view_finally_launches_in_ger.html.

because I do not understand what it means and I do not know what its implications are. I may be able to do two or three moves in a chess game, but the stuff that I am reading is fifteen chess *games* ahead where I am now. I am tired. You say "choice," but I have no choice. If I want to participate, I have to say okay or not install the stuff. Of course you will tell me: "Well, you should not have installed it," but what kind of choice is that? To play or not to play? What is "choice" in this day and age of privacy? Forget about it. Is that what we are in for?

DR. FAIRFIELD: Some of my colleagues might just say: "Do not install the software." I would say that you just described the set of terms under which the law would deem the contract unenforceable. That is pretty close to how California law treats unconscionability. You have no choice and you cannot read it. I would take a different approach than California. California laws are very forward leaning on this topic. We have seen a number of cases that have been knocked out on end-user licenses based on exactly the same argument you just made. That is a fact, but I guess it is probably the wrong take. A better take might be in between the take that says: "You are bound by whatever arcane stuff we put in page nineteen," compared to the take that says: "Just because you clicked 'okay' does not mean you really gave consent to anything." You did give consent to something. The famous law professor Karl Llewellyn provided a way to look at this when he said that we give specific consent to terms that are sort of put up under our nose in flashing lights.[29] That is frankly where our law on privacy should be. With respect to the rest of the terms, we give consent to a blanket, standard deal—which is the theory of blanket consent. It would be sort of a tragedy if you had to read the whole thing. We are not going to make you read the whole thing, but we will bind you to the whole thing as long as it is not too spooky.

My guess is that there are currently three sets of courts with differing viewpoints. There is one set that is going to bind you to anything that is expressly set forth in a legal document—which is basically the Virginia courts' interpretation. The California courts are going to knock out anything you have no choice over on the grounds you just raised. I think the rest of the country is likely to do something closer to what I described and will only really enforce anything you make users read and then click "okay." There are ways of having check boxes and ways of really bringing one or two lines to somebody's attention, which is going to be pretty ironclad. As for the rest of the terms, no one is going to read them. The court knows no one is going to read them, but they will enforce them as long as they are not spooky.

MS. ARCHIE: Just to give a real-world example, Facebook has made a substantial amount of changes following the Canadian Privacy Commissioner's report of a Toronto professor that did a take down on the site.[30] The

29. Karl N. Llewellyn, THE COMMON LAW TRADITION: DECIDING APPEALS 370 (Little, Brown and Co. 1960).

30. Elizabeth Denham, Assistant Privacy Comm'r of Can., REPORT OF FINDING INTO THE COMPLAINT FILED BY THE CANADIAN INTERNET POLICY AND PUBLIC

report really focused on apps and how there was zero disclosure and no presentation of terms. Facebook has been working on that aspect of their relationships with users and their app developers for a long time. Now it is a deterrent because currently when a user logs onto Facebook, a window pops up and informs the user of what Facebook is going to do and how it is going to access data. You get a better level of notice than what you are describing. It tells the user not to necessarily focus on the unexpected, but on the really important stuff. Facebook tells the user: "We are going to collect these six categories of data, do this with it, and share it with other people." I think it is on the developers to put that notice in there and to do better than what they are doing.

I was smiling as you were describing your personal experience because I thought it sounded like every conference Berin and I have ever been to, or every FTC report I've read. This is the conversation that is going on in Washington. The Republicans have the Energy and Commerce Committees now on the House side, and I do not know how fast they are going to move on privacy. I know Chairman Rockefeller and Chairman Leahy on the Senate side both care a lot about this issue and are going to try to do more. They will either bully pulpit businesses into improving on what you are describing, or they will haul in key public-policy players in Washington D.C. and put heat on them to do better. The chairmen will tell them: "This is not good enough. We are getting heat from our constituents. Fix this or we are going to regulate." "Fix this or we will regulate" is the climate in D.C. right now.

We have not talked about the "do not track" browsers that are starting to roll out with actual functionality. The FTC has basically said that if you do not roll these out, we will go nuts on the Hill and get permission to legislate "do not track."

PROFESSOR NGUYEN: Is that what I am going to tell my CEO who does not want to hear anything about privacy because he wants to make a deal? Has it not been a threat for quite some time to tell him that right now the climate in D.C. is "fix it or we will regulate?"

MS. ARCHIE: It has been. Your CEO might be right and he is paid to make big business judgments. The board, senior management, and leadership of the company make those types of business judgments and risks. They get in trouble when they do not consult, think, and weigh privacy—whether they have a big slip up in judgment or have fair judgment. These are absolutely gray areas in matters of judgment. I do not fault anybody if they come out in a way that shows they are trying to build a business. I find that most people are good and very few want to go out and break the law.

MR. SZOKA: Another way to put what Jennifer is saying is that law is really a blunt instrument. Most of this does not come down to what a court will do, even though sometimes there are scenarios where that is the issue.

INTEREST CLINIC AGAINST FACEBOOK INC. UNDER THE PERSONAL INFORMATION PROTECTION AND ELECTRONIC DOCUMENTS ACT (2009), *available at* http://www.priv.gc.ca/cf-dc/2009/2009_008_0716_e.pdf.

For the most part, it is about something as whimsical as what does a reporter at the *Wall Street Journal* or a staffer who works for Senator Rockefeller think of you. Are you likely to get called in when there is a hearing on privacy practices in the video game industry? What does it mean—not just for your brand, but for your CEO's brand? Tell your CEO: "You know, Jerry, you are going to be in this business for a long time. Have you thought about what is going to happen if your name is in the *Wall Street Journal*'s story?" It could be any number of smaller outlets. All of these things are ways in which the government and other people who are—to use Josh's term—forward leaning on privacy are trying to push forward on technology, user expectations, best practices, and the law in the broadest sense.

I think when people look at this they often have a sense that this is all about courts and regulations. But it is really more about subtle pressure, intimidation, and—sometimes—outright extortion by lawmakers and attorney generals. It is just not as simple as what a court will and will not do. The answer to your question, Professor, is that you really need to try and be as forward leaning as possible. You want to stand out. You actually want to be in the *Wall Street Journal* as an example of a company that is doing the right thing because that reflects very well on you and the people in your company. It is a good story you can tell to your investors, advertisers, and all the other companies that are attached to and value your reputation.

MS. ARCHIE: I see so many different types of questions related to diligence that come from possible business partners, big investment banks, and small private equity groups. This is not an overlooked topic anymore. And there is no bigger buzz kill than the paragraph that says: "On this date we received a civil investigative demand (CID) from the Federal Trade Commission," because everyone knows it is a cloud. It could easily take fifteen months to get producing documents and depositions to resolve the issue, and it is going to end with a consent decree. Every single consent decree is a public document that is filed and quickly will become a top search result on the brand. It is not a fun position. And it is a huge buzz kill as a startup company to be the one that is dragging around the FTC CID, even if you can defend it.

MR. SZOKA: Another way to tie this into the conversation we were having about this earlier is to say to your CEO: "Wouldn't be a shame if the work of art, or this business, or this thing which you have poured so much of your time and effort into, got tanked because we had to put a paragraph like that into all of the legal language that went out to all of our deal partners?" Also, mention the fact that anybody can Google the name of our company and find you, which is what you want to avoid. Those are strong incentives that exist even in the absence of the written law or what the courts hold as the right thing.

AUDIENCE QUESTION: Is there a distinction in the law regarding the practice of more benign privacy issues? All game developers want to build in a level of telemetry to determine where players are going and what they are doing. Developers do not care about privacy and just want to know that

ninety percent of people failed at that this level and do not care about private information. Is there a distinction between the naked commerce side of privacy as opposed to the more benign design in private-development reasons?

DR. FAIRFIELD: A lot of this has to do with the monetization model, which is directed and targeted advertising requiring that you know a lot about the person at whom you are targeting the advertising.

AUDIENCE QUESTION: Independent of the platform.

DR. FAIRFIELD: What you are talking about though is something different.

AUDIENCE QUESTION: Right.

DR. FAIRFIELD: Generally, the difference will keep you out of trouble. As long as the data is hashed, aggregated, and not individualized, I cannot think of any way you would get in trouble.

MS. ARCHIE: It is okay when you are not marrying it to a user ID or some internal unique identifier.

MR. HIRSCH: Ideally, we want to marry it some type of demographic information, but not to a specific ID.

DR. FAIRFIELD: As long as that is hashed out or just dropped out, and you have the aggregate data, it just is not an issue.

MR. HIRSCH: Good to know.

MR. EHMKE: Be careful that it does not transform away from that.

DR. FAIRFIELD: Exactly. There is the drill-down problem.

MR. EHMKE: It is easy to go: "Well gosh, I have this really big database of good stuff. I wonder what I can do with it."

MS. ARCHIE: The other issue is with inadvertent collections. Nobody at Google was having round table conversations reminding its staff not to forget and pick up the packets from the houses as they drive by. Nobody talked about it, thought about it, or stopped to question why IP addresses were collected when they were not needed. In real business, it is important to plan for the future, so you are not always cleaning up after the parade. The problem is not usually a malicious grab for user-base information by deceiving them with what you are collecting.

MR. EHMKE: Another issue may arise when a different arm of the company collects the data. You meet with the people collecting the data and discuss that it will not be used—except internally—because there are rules in place. You think you had a great meeting, but then six months later a different arm of the company asks: "Hey, what is that?"

MS. ARCHIE: I tell my clients if you are the legal guy, chief privacy officer, or the one who speaks to the CEO about privacy responsibility, at the end of the day you are accountable for the description of the data that is collected and how it is used. So what are you going to rely on? First, I give them a mini Sarbanes-Oxley lesson.[31] Then I tell them: "Make the studio sign

31. Sarbanes-Oxley Act of 2002, Pub. L. No. 107-204, §§ 404–409, 116 Stat. 745, 789–91 (codified as amended in scattered sections of 15, 18 U.S.C.) (2002).

off. Do not let them send you some half-baked e-mail that is full of gobbledygook. Explain to them that they are the authors of this game and they are responsible to the heads of the studio to say what data will be collected. Get them to sign off on it, so at least you have that estoppel. If you are really mad at somebody later, you can point to those signed papers."

DR. FAIRFIELD: Problems like that happen more often than you think. In the game- and product-development process, if you are running metrics, you often start by grabbing all the data you can get and then later decide how to use it. The fact that it was gathered means that some other person, in some other capacity, may well find a use for it. I have seen this more times than I can count.

MR. SZOKA: Including law enforcement.

DR. FAIRFIELD: Especially law enforcement. You do not need it but grabbed it because it was there and because you might have some purpose for it later down the road.

MS. ARCHIE: One thing that I neglected to cover is "delete and destroy." You are in the development stage, and you have old databases full of information before it was hashed that were never taken offline. It is common because it takes a lot of cycles to properly delete and destroy data. This is a really key component of privacy by design. The cheapest thing is not keeping it in-house because no one gets around to the destruction schedules except if litigation was filed.

DR. FAIRFIELD: Actually, do seek counsel on this one because delete and destroy has gotten really touchy since Sarbanes-Oxley.[32] You need to have a corporate plan in place that is strictly followed. There cannot be the least inkling that you are destroying data because you do not want somebody else to see it. It has to be absolutely routinized, and if litigation is filed, stop and consult an attorney. Do have that policy in place.

MS. ARCHIE: The e-discovery rules are brutal. I settle cases every day that I would not settle but for the burden of that step in the process. You want to pick a point on your risk profile. Do not pick summary judgment because that happens after e-discovery, where an outside vendor comes in and everybody has to sit down and meet with the lawyers personally. It is a very disruptive and painful process.

MR. SZOKA: In other words, think more about how journalists would react to what you are doing. That would be more of the standard you have in mind.

DR. FAIRFIELD: Are you shredding documents because you do not want someone to get their hands on them? You need to stop. Are you destroying things on a regular basis just because you do that at the beginning of every month? That is absolutely fine. Just have it in writing and follow your schedule.

---

32. *Id.*

PROFESSOR NGUYEN: Since games are global, does that mean privacy is global?

MS. ARCHIE: Unfortunately. I think I called something else devilish, but this is the other devil in room. There has been an attitude for a long time that—since our servers are in the U.S. and you came to us—we will put a paragraph stating that, if you choose to come here from the E.U., or another more restrictive country, you have made this choice yourself. Nothing about that statement helps you, except it is good to have it there in case someone ignorant in the U.S. reads and evaluates that it is there. Sometimes, the dumbest thing people do is simply put the words in that they are Safe Harbor compliant when they have not done any of the necessary steps. Everyone has heard there is this thing called the E.U. Safe Harbor, so they think that because they have good policies they are Safe Harbor compliant. They intend to get there, but they go ahead and put themselves on the list before they do. There is a string cite now of FTC enforcement actions, which is the first wave of policing Safe Harbor. If you are collecting money—and many games require a monthly subscription or virtual goods purchased one at a time—there are very different rules about refund and cancellation policies. It becomes a very complex legal environment when you start taking credit cards, and laws vary among the states.

I do not know of a game that does not put cookies on a computer because that is how you play. In the E.U., it seems to be a very subtle and accepted view in their view, and that means that if a cookie is residing on a P.C. or an Apple computer or whatever kind of mobile device in the E.U., then you operate and use equipment. You can wink and nod and ignore that fact for only so long before you get on their radar. There is a galloping awareness among all of the separate data-protection authorities. Unfortunately, they are like our federal system and are not uniform. There is no such thing as E.U. law on data protection. It is still something that needs to be sorted out.

Another global issue that often comes up is that you can tell from a user's IP which country they are coming from, and in our country there is a list of countries we are not allowed to take money from. The U.S. government is now focused on this issue because there are very strict laws. Companies need to have a basic knowledge of which countries, such as Sudan, are on the block list. International users can cause issues when building in a purely web-based environment. It is overwhelmingly true if you are knowingly distributing in a shrink-wrap environment.

MR. EHMKE: Another area that gives me nightmares to think about is when a company has a large distributed system with different game players all over the place. This type of system involves housing servers in different countries, but it is all part of a single distributed system. All of a sudden you realize that data is being transferred from this country to that country automatically, which is triggering different privacy laws in all the different countries where the data is transmitted. It still gives me nightmares thinking

about the different ramifications of just sending data around as part of the back-end operations of your game or process.

PROFESSOR NGUYEN: Are there any more questions from the audience?

AUDIENCE QUESTION: In relation to what Andrew just said, how do you compromise that with a situation like the law China passed sometime last year that requires people running online games in their country to have a registration system that keeps the contact information of everyone playing on their systems?[33] It is a local issue since it was just serviced in China, but how would you deal with a situation where a game has to abide by China law since it will incorporate people from China? Now, you are keeping more information concerning Chinese players on your system than you are from U.S. or European players.

MR. EHMKE: As Jennifer was saying, there is not a global rule set. Just like in the United States, there are fifty states and there are fifty sets of laws. Privacy has become more of a federal issue here. I do not know if that is a good or a bad thing. If you start doing business globally, you are going to have to know each country's rules because every country has its own laws. The question now is what you should do in China or what you should do in Taiwan, as opposed to the things you would do in South Korea or the United States. You are going to start blending each law until you find the lowest common denominator. You are not okay just because you are abiding by the China rule because the China rule is going to be different than the U.S. rule and different than the South Korea rule.

MS. ARCHIE: In essence, investment banks and diligent investors are already onto this issue. The requirements and warranties do not just say it complies with U.S. law, but instead say it complies with the laws of the jurisdictions that apply to the business. You can find that you tripped some clause and put yourself in a contract situation.

MR. SZOKA: There is also an important moral and brand protection dimension to consider because you have to make a moral choice as to whether you are going to do that. Google had to make a decision as to whether they were going to continue to play ball with the Chinese government or not.[34] You guys build games, but what you are really building is another communications platform. And any communications platform can be used by Al-Qaeda dissidents or for a business meeting. We could be having this meeting in *Second Life*. If you are a government like China's government, there are reasons why you want to keep track of that information. There are also reasons why the U.S. government would want to go to

33. *See* Michael Kan, *Chinese Online Game Law Requires Real-Name Registration* (Aug. 2, 2010, 3:40 AM), http://www.pcworld.com/printable/article/id,202332/printable.html.

34. Kim Zetter, *Google to Stop Censoring Search Results in China after Hack Attack*, WIRED (Jan. 12, 2010), http://www.wired.com/threatlevel/2010/01/google-censorship-china/.

some of your companies and ask you to turn over user data. The government might ask where your users have been in the site, because they think Falun Gong had a meeting in the virtual world. You must decide if it is as simple as asking: "Do I comply, or do I really want to offer my service there?" Can you sleep well at night knowing that the information you turn over will be used to put people in jail, or maybe even worse? Do you want to have to deal with the journalists or the Hill staffers—especially with a Republican Congress that is more likely to care about this—who haul you in and question you about turning over data on what your users are doing and how that led to Falun Gong members being arrested? It is not an easy question, but it does also fall under the umbrella of privacy.

MS. ARCHIE: The take away is for companies to be intentional about their interactions with foreign players. Also, it is important to be aware when you start to build up a critical mass of traffic coming in from the E.U. that you might end up tripping over data protection in another country. There are trip wires you can set up to inform you when a pre-defined critical mass of players has been reached.

MR. SZOKA: This is about being conscientious. It is about a certain kind of Zen about living an examined life. It involves carefully examining what you are doing in your business, what data you are collecting, whether you need it, and under what circumstances are you giving it to others, including and especially governments.

PROFESSOR NGUYEN: I think with that, we will end. Thank you so much to Jennifer, to Andy, to Josh, and to Berin. Thanks to the audience as well.