CARLTON FIELDS

S1:E3 - Even the Games Have Eyes: Data Privacy and Gaming

CYBERSECURITY AND PRIVACY | ESPORTS AND ELECTRONIC GAMING | MEDIA, ENTERTAINMENT, MUSIC & SPORTS | TECHNOLOGY & TELECOMMUNICATIONS | MARCH 13, 2019

Steven Blickensderfer

Nicholas A. Brown

Steve and Nick take a deep dive into the emerging legal issues surrounding data privacy in gaming. They discuss the history of data collection in games and how that data has been used, and explore some of the regulatory restraints and challenges facing industry players. Then, in the 1v1 Showdown they debate various approaches to regulating these sensitive issues.

Transcript:

Nick: Welcome to the LAN Party Lawyers Podcast, where we tackle issues at the intersection of video gaming, law and business. I'm Nick Brown and with me is my co-host and partner in crime, Steve Blickensderfer.

Steve: Hey there, Nick.

Nick: Before we get going, we just want to remind everyone that nothing we say here is legal advice. What are we going to talk about today, Steve?

Steve: A topic very near and dear to my heart and that is data privacy regulations in video games and video game development. So to give you a roadmap of where we're going, first we're going to talk about the various data privacy regulations impacting companies in the gaming space—things like the new European data protection law the GDPR, California's new data protection law the CCPA and others. Then we're going to explain why the increase in data privacy regulations is becoming an increasingly big deal for video games in the esports industry. Then we're going to do a 1v1 Showdown where Nick and I will debate various approaches to how data privacy regulations could be implemented whether on a federal level, state level, a mix of both, or not at all, and then we're going to share some takeaways and wrap up.

Nick: Alright so we've got a lot to cover today. To start, what is the difference from a high level between data privacy and cybersecurity? Because I always see those two things thrown around together.

Steve: Okay, so take cybersecurity, think of bad actors doing sneaky things to get your data.

Nick: Okay.

Steve: Contrast that with data privacy, and that refers to the laws and regulations that cover around the collection and processing of data.

Nick: Okay. Now today we're going to talk about the latter, which is data privacy—but we have another LAN Party Lawyers episode dedicated just to cybersecurity.

Steve: That's right.

Nick: Well before we get going, let's get some context. Here, it all started, believe it or not, with Space Invaders. In the old world of video games, when you go to an arcade, developers didn't have any real ways to interact with players after the game was released. They couldn't get any info, they couldn't interact, they couldn't see anything about the metrics of what their players were doing; they would just shoot the game out into the world and that was it. Space Invaders came along and it was actually the first game to store your high score, which doesn't sound like a big deal now, but when that came out it was revolutionary. And it also allowed users to enter their initials to announce their high score to the world, so that was the first data collection in gaming. So fast forward, then the internet came along and then people started having LAN parties where they would get all their computers in the same house and create a local area network, that was how if you wanted to play Doom or Wolfenstein with your friends for example.

Steve: Mechwarrior.

Nick: Or Mechwarrior, that's how you would do it, and then later on we got the high speed internet that we're all used to now that brought along a real online revolution in games. So now the games industry is increasingly data driven, and there's a constant two-way dialogue between developers and their players. Games nowadays can—and many do—capture and log all sorts of information about the players' interactivity. So every single action taken, every decision made, every communication players make, can be logged and saved by the developers whether the players know it or not. Now sometimes this data is used for everyone's benefit in a benign way, for example, developers can analyze how many players access certain content or use certain features and that helps them determine how and whether to develop going forward and how to spend their resources. So one good example of this is that Bioware, the makers of the Mass Effect series, they had access to see which conversations in the game their players were skipping over. And that allowed them to figure out what characters in the game people wanted to listen to and then they were able in future installments of the game and in DLC to divert resources appropriately. If nobody's listening to this character, then we probably shouldn't pay a bunch of money to get a bunch of unique voice acted lines in the game, we should focus on other areas where players actually engage.

Steve: And for those people that don't play that game, this is a game where you select "A" if you want a certain type of reaction or you want to respond in a certain way and the voice that would come after that would be something different depending on what you chose.

Nick: Exactly, this type of data can also help reveal bugs or confusing user interfaces—if you have a game that's being played by millions of people and nobody's been able to turn in a certain quest or mission, then it may be revealing the fact that there's a bug with that and people aren't doing it only because they can't. And that type of data allows developers to figure out where they need to go to solve problems.

But at the same time, this data can be used for less altruistic purposes, for example, trying to figure out what makes it most likely that people will spend more money on your game, and they can figure out how to maximize monetization, they can figure out how to get more microtransactions in front of you that you might be likely to purchase. Or perhaps even worse, this data that's gathered itself can be sold to third parties with who knows what their motivations are. And so, of course, as a result there are a bunch of laws and regulations at play and that's what we're talking about today.

So Steve, tell us, are privacy laws in the U.S. organized in a certain way that affects gamers here?

Steve: Sure. So to compare the U.S. to other countries like in Europe or even maybe in Latin America, privacy laws in the United States are organized more by industry than anything else. So you have laws that regulate the healthcare space, that would be HIPAA and HITECH; then you have the banks and the financial sector and those would be governed by Gramm-

Leach-Bliley Act and the Fair Credit Reporting Act; then you have the education space that's governed by FERPA. In addition to industries, you also have certain user groups that are protected and one that really sticks out are children, and the use of children's data is governed by the Children's Online Privacy Protection Act or COPPA. So that's a general overview of how the privacy laws are organized in the United States.

Nick: Alright well is there a law that specifically regulates the video game industry then?

Steve: No, there's no particular law that just governs the video game industry itself.

Nick: So what actually does end up regulating the video game industry if there's no law specifically designed for that?

Steve: Everyone engaged in trade and commerce is regulated by the Federal Trade Commission (the FTC) and the FTC Act. More specifically, Section 5 of the Act says that you can't engage in deceptive or unfair trade practices, and with respect to video games, you can say you can't engage in that kind of activity with respect to data. So everybody in that respect is governed by the FTC and Section 5 of the FTC Act. And aside from that, there really wasn't an overarching data protection law that applied here in the states across all businesses, much less worldwide, that is until...

Nick: Until recently.

Steve: ...2018.

Nick: Yeah.

Steve: 2018 some would say is the like event horizon for data protection and privacy regulation.

Nick: I'd say that.

Steve: It was huge, and there are many reasons for this. First and foremost is Europe's data protection law, the GDPR, went into effect in May of 2018. And this law has had a global reach, which the previous law that it replaced didn't—it effects all businesses and technologies that collect and process personal data which we will explain in a little bit. That's the GDPR.

Then we have California, which passed the California Consumer Privacy Act which is similar but very different in many respects, one of them being where the GDPR took years to develop, the CCPA came together pretty quickly. One similarity is that they both have a global reach to protect processing of data of California residents.

And then to give another example of how big 2018 was, another large economy, Brazil, passed a data protection law in August of 2018 in Portuguese, I don't how to say it in Portuguese but the acronym is LGPD. So that's another huge law that happened in 2018.

And as we enter 2019, it looks like none of that inertia has stopped, it's just still going. Washington state recently has introduced legislation to regulate data processing called the Washington Privacy Act.

Nick: And if I'm not mistaken, Congress is considering federal legislation as well, right?

Steve: That's right and that's really the biggest news of 2019 so far is where are we going with Congress regulating it, how much are they going to regulate and we're going to get into that a little bit in our 1v1 Showdown. But suffice it to say Nick, there's an abundance of new laws regulating the collection and processing of data.

Nick: Sounds like it.

Steve: Including video game and mobile game data affecting businesses all over the world. Now, let's talk about what kind of data is being regulated, not just any data...

Nick: Okay.

Steve: ...personal data.

Nick: What does that mean?

Steve: Personally identifiable data or personal information. It depends really what act or regulation we're talking about, some statutes are in the middle of the road when it comes to the definition of personal data. Let's take the GDPR for example. In the GDPR, personal data includes data that can be used alone or in conjunction with other data to identify someone. So let's take your height and your weight separately, that doesn't say anything about you, but we add your name to that, boom, we've got something personal about you. Your name itself would be personal but this is showing the name, or the height and weight ...

Nick: Connecting all that together makes it more personal.

Steve: Exactly. And then we have the California statute which has a very broad definition of personal information and that includes any data that can be reasonably linked directly or indirectly to a person or household—and that's new, adding household to the definition. So we're talking about geolocation data, behaviors, attitudes, Nick, when you've got a bad attitude.

Nick: The California statute covers my bad attitude?

Steve: Yes, it does. Your olfactory information.

Nick: It's how I smell?

Steve: That's your sense of smell, so if you don't have one that would be pretty personal and California regulates that. But putting it back into context where we are talking about video games, importantly, personal data can include electronic data. Take cookies, for example...

Nick: Delicious.

Steve: ...cookies are delicious, but we're not talking about those cookies, we're talking about little log files placed on your computer by websites, for example, that help to improve your experience by recording your browser type, language, which kind of operating system you're using.

Nick: And that's covered by the California statute?

Steve: It's also covered by the GDPR.

Nick: Wow, okay.

Steve: To the extent it helps to identify you. Again, you have to put that into context and follow the definition under each statute. But the California statute goes even a step further, and it says your browsing history is personal information...

Nick: Really?

Steve: ...your search history, which I know your search history is pretty personal.

Nick: Incredibly.

Steve: Yeah, totally. And even a consumer's interaction with a website is considered personal information. So why is all of this important? Let me tell you, Nick. It's because these recent laws, in the context of gaming, modern games generate a tremendous amount of personal data.

Nick: I read a factoid—and tell me if I'm right or wrong about this—but that certain big publishers generate upwards of 6 terabytes of personal data a day just from video games.

Steve: That's incredible. Yeah, it just goes to show you, I don't know if there's enough awareness out there as to how much personal information is generated by video games. So why don't you walk us through what types of information is generated.

Nick: Sure. So it depends on the video game, right? You know, back in the old days of Nintendo, it would only save game data, you know, the number times of you've played, your saves, how far you've gotten, so there was not a concern that the data you generated by playing the game was going to get sent to Nintendo or someone else for any kind of analysis or other use.

Steve: Which cookies you like to eat.

Nick: Which cookies you favor. But now, things are totally different and you'd be amazed what can actually be sent. So one example: in addition to all the actual game playing data that we mentioned earlier, you'll recall a few years ago Xbox came out with a little camera controller called the Kinect, and what it would do is it would actually take a video of wherever you set it up and you could control the game, it would capture your movement, you could control the game with your movement and control other functions just with your voice. And that controller, that interface would record and gather a bunch of the players' physical characteristics, including facial features, body movement, and voice data.

Steve: You know, I looked into the Xbox old privacy policy and it actually called that information "skeletal tracking," which I thought was pretty spooky.

Nick: Yeah, that's a little weird. But in addition, other games can get your location and your surroundings. One good example is the Battlefield series has a feature, they do a lot of stat tracking, one feature they offer is that you can compare based on your IP address and other playing information, you can compare not only your stats against the global leaderboards but you can also compare it against other people in your own geographic area. So I could see if I was doing better or worse than other people in Tampa, Florida, where I was playing, or in Florida or the United States or the whole world.

Steve: I think that's pretty neat.

Nick: It is pretty neat, except I usually did worse. But other games will gather your surroundings or biometrics and other information that especially glean from your social networks, if you hook up Facebook or one of your other social networks to one of your gaming tags, which is growing popular now. You also have to consider mobile games; one interesting example is that we heard the NSA is apparently watching you when you play Angry Birds.

Steve: Mm-hmm.

Nick: According to docs that were revealed from Edward Snowden, the NSA used Angry Birds to collect phone numbers, e-mails, and user device codes.

Steve: Scary stuff.

Nick: Yeah, I also don't want them to know how bad I am at that game. Another really good example that maybe makes a little more sense would be Pokémon Go. So personally, I play Pokémon Go. I have never played a Pokémon game in my entire life until this game.

Steve: Not even on the GameBoy?

Nick: Not even on the GameBoy. For some reason, it's a franchise I just missed. But Pokémon Go came out on mobile platforms in the summer of 2016, and it got a lot of buzz, a lot of fanfare, and a lot of controversy because of some of the information it collects. So basically, for those of you who don't know, you play it on your phone and it's a modernized, updated version of the old Pokémon games where you would go around and collect these little creatures you find out in the world and you could build out a collection, you could improve them and evolve them and you could even have them battle. And Pokémon Go allows you to actually do that out in the world when you go places, you can catch these things and build out your little collection. And to do that, the game superimposes the graphics of your character and whatever Pokémon you find, over the real world maps and with real world weather data of where you are and so in order to function properly the game has to record your location via GPS tracking. So it collects your geolocation data, among other things that your cell phone would already be gathering.

Steve: But that game got in trouble for collecting more than just that. It actually collected Google profile information. Why does Pokémon Go need to collect that information in order to deliver a quality game?

Nick: You'd have to ask them, all I know it is a quality game.

Steve: In addition to the information that Pokémon Go collects and some of those other games, in-game data could reveal a lot more, and this is where it kind of gets a little darker. Video games could also get very personal, [they] could reveal your temperament, how you react, what fears you might have if you jump in a certain game at a certain point if that causes you fear, your leadership skills depending on maybe what traits you select in game for a character, and even your political leanings.

Nick: Right so there was a guy a few years ago who came up with a theory that you could learn a lot about a person's personality just by watching their in-game behavior. So, not necessarily based on your statistics or whatever you chose, but certain activities and certain behavior by players was associated or correlated with certain personality traits, if you believe the theory. And so that's how, by taking this game data that other people are just shooting into the game, they can extrapolate from that and some people believe that you can tell a whole lot about a person, not just their gaming traits.

Steve: And so what's the goal of all this? What's the goal of collecting all this personal information?

Nick: Well it's twofold, right? On the one hand they can make better games, they can learn where players are engaged, where players are not engaged, what types of features players like, what type of interfaces work and are confusing or are clear and intuitive, but also, as we said, it's a good way to find out where and how people are more likely to spend money.

Steve: Okay, Nick, I think it's time. It's time for the 1v1 Showdown.

Nick: Alright, excellent. Now, this is the part of the podcast as everybody knows where we take the issue of the day and have a mock argument. We assign each other different positions and face-off. Today, we're going to be debating the different ways that data privacy regulations could be implemented in the U.S.

Steve: That's right, Nick. It's really no point in debating the con and pro in saying we shouldn't have any data regulations, because I think that's where we're going. So instead, what we're going to do is we're going to debate how best to implement data privacy regulation. So we're going to say let the states do it, let the federal government do it, let them both do it, or let the market do it.

Nick: Alright, Steve, what's up first?

Steve: Nick, I'm going to start us off with this: states should be free to regulate data protection themselves. This is the classic Tenth Amendment argument, or position, and I'm quoting from the Tenth Amendment of the U.S. Constitution here: All "powers not delegated to the United States by the Constitution, nor prohibited by it to the states, are reserved to the states, respectively, or to the people." Privacy, if it is to be regulated at all, is a day-to-day governance responsibility that states should bear. The federal government should mind its business and let the states take care of the data processing practices of their citizens. Justice Brandeis said it best, Nick.

Nick: What did he say?

Steve: The states are laboratories of democracy where we try novel, social and economic experiments. Let the states work on different variations of data privacy laws so we can figure out what works best, because there's a lot of different debates and confusion as to what's the best approach here. Eventually, what we'll see is that the best—the cream—will rise to the top and eventually be implemented across the board. That's what we saw when California adopted its first ever website privacy policy regulation, CalOPPA—C-A-L-O-P-P-A for those taking notes at home. That's why we first started seeing website privacy policies become common place.

Nick: So it's California's fault?

Steve: It's California's fault and now they're following it up with the new California statute so they're going to change the game as we move forward. So at the end of the day, Nick, what works best for residents of California, may not necessarily work best for Floridians or Washingtonians so that's why the states should regulate data privacy.

Nick: Alright, well Steve you must have skipped a few constitutional law classes in law school because I'm going to explain why the federal government should set a single standard that preempts state laws.

Steve: You knew I was there.

Nick: As we all know, interstate commerce is the federal government's business and as we learned in con law, a guy growing wheat in his backyard affects commerce enough to make that the issue of the federal government, not the states. And so if growing wheat in your backyard is enough, then certainly selling games—including these monster AAA behemoths—is enough to affect interstate commerce and put this in the hands of the federal government. The gaming industry in particular is not in any one state, even though it may be, you know, more popular in some states than others.

Steve: I'd beg to differ with Farming Simulator; I think that's only in some states.

Nick: Well fortunately they can send that and sell that game anywhere they want; it's a worldwide phenomenon. So the federal government can and should regulate this. As a practical matter, how can you have different laws by state that apply to video games? You don't release a game in one state only, once it's online, it's everywhere. So state-by-state regulation would mean that the most restrictive state rules everyone because game developers would have to make them compatible with their rules from that one state and that would apply across the board. So it's better for businesses to have consistency across the board by having a federal standard, businesses already struggle and innovation is stifled when there are too many different and sometimes inconsistent regulations that need to be met. For example, you've got one state that says you have to disclose certain information, you have another state that says you can't disclose certain information—it would be really difficult to comply with both, if not impossible. It's already difficult enough to comply with laws country by country; having all 50 states weigh in with their own little perspective would only make it worse. So I've got to say at the end of the day, some things are so important you should not encourage variation. Consider COPPA, for example, which you brought up a minute ago, which regulates the use of children's data, that statute preempts state laws—probably because protecting kids' data is not something we should be testing in your little state laboratories.

Steve: Alright, Nick, fine—if the federal government is going to get involved, it should at least permit the enactment of stronger state regulations and I'm going to tell you why. And what I mean by that: let the federal government pass a law that creates a minimum standard, let's say the floor, and let states have room to create more exacting standards if need be, the ceiling. So don't preempt states from having the right to govern themselves if they would like greater data protection for their citizens. So this is how Gramm-Leach-Bliley works. California is pretty famous for its Financial Information Privacy Act, and because Gramm-Leach doesn't preempt state laws, California was able to come out with a statute that offers greater protections than Gramm-Leach by increasing disclosure and notice requirements before processing and sharing data. The Fair Credit Reporting Act is another example where some states have their own statutes that require opt-in consent before certain data can be shared by financial institutions. Some games, take Pokémon Go which you talked about a minute ago, target and collect information from children, and parents may not be aware of what data and information their kids are giving game developers. That's why allowing states to pass tougher regulations can help. And as I said before, what works in one state may not necessarily work in another state. So we should let states decide what works best for their own citizens. The federal government doesn't explicitly treat—and this is another point—the federal government doesn't explicitly treat privacy as a constitutional right.

Nick: It's implied.

Steve: It might be implied from the Fourth Amendment, but states like California and Florida actually write it into their state constitutions, which arguably maybe they treat privacy a little, you know, more of a fundamental right. So that's another reason why states should be allowed and the federal regulation, whatever, shouldn't preempt. In a word Mr. Brown: Don't tread on me.

Nick: Wow, okay well by my count that's four words but I'll let that go. However, I will say you've convinced me, I've changed my mind; let's not have any regulation—all the way against the other side. No regulation whatsoever let the market decide, capitalism at its finest.

Steve: Wow, coming from you, that's pretty big.

Nick: Listen, overly restrictive regulation can hurt business and in this case game development. Okay? You don't want to stop getting these great games just because they have to tip toe around the privacy laws. You know, and I'll say Pokémon Go gets unfairly singled out; it's hardly more dangerous to you than carrying your smartphone in the first place. As we all know, your smartphone can track you any time it wants, owning a cellular phone in your name instantly diminishes your privacy whether or not you have games on it, because most mobile devices can be tracked whether or not they're powered on by the carriers' cell towers. And so you might as well go ahead and fill out your Pokédex if you're already giving up your privacy by having a cell phone. In the end, it is your responsibility and mine to protect your own data; it's a personal responsibility issue. There are things you can do or parents can do for their children to minimize their data being collected by games and the government shouldn't come in and tell people what they can and can't do. The games that are better at allowing people to do that, to manage their own data and to know where it's going, those are the ones that are going to excel in the marketplace. If people don't want the benefits of these games, nobody's making them play, if you get scared because you don't know what a game is going to do with your data, just don't buy it.

Steve: I'm not scared, Nick.

Nick: I hope not. Not all developers, even at the end of the day, use this data for bad purposes. Player data is generally utilized to make games better, it finds out where the holes are, where people want to go and where resources should be diverted. It improves game mechanics and features and removes bugs, and for those companies who do mishandle data or do nefarious things with your data, people are going to find out about that and they're not going to be very popular. And so let the market take care of that too: survival of the fittest, we should go with the ones that handle their own data best and everyone should be in charge of their own.

Steve: Wow, I'm glad this is being recorded. Nick, the robber baron! That's a pretty bold assertion, in fact the boldest assertion I've ever heard from you.

In the end, we don't know how all this is going to shake out, Nick. Congress is considering a number of variations and states continue to introduce new statutes but there are a number of things that developers and gamers can think about going forward.

Let's start off with developers. Okay, so some takeaways for developers, I think we are in a very exciting time for privacy in that it's really top of mind for consumers. So one thing that developers can do to really stand out among their competition is to think about and maybe set their brand, their product apart by thinking about privacy implementing in their game, being transparent with their data collection practices. What does that mean? Writing clear, plain English, privacy policies and terms of service, also, taking privacy and implementing it into the design phase of games.

Nick: So think about from the start; don't think about it as an afterthought.

Steve: Exactly, every time you have a new game maybe one of the things should be what kind of data are we going to collect? Maybe we shouldn't be collecting everything—like for Pokémon Go, maybe we shouldn't be collecting Google profile information, that's the step too far. And that would maybe avoid press issues or whatever that come later. But I think just having that implementation in the design phase is what's key and that's what helps to design a game that's maybe more data privacy-friendly. And other things that can be done, know the regulations and the various data protection laws that may apply and may affect the business, which again, it's pretty tricky in the United States because of the way that privacy has grown up, the privacy regulations are just kind of sectorial.

Nick: And it's going to change over time, right? What's true today with respect to the privacy laws may not be the case in another year or two.

Steve: That's right. It's really a Brave New World when it comes to data privacy in the U.S. And also, another key thing before we move on to gamers is to understand the compliance is not going to happen on day one. Compliance is like getting on the road and starting a marathon, it's a process and every day you're working towards getting closer to that 100% compliance goal. And so just understanding it's a process and the regulators know that and it's just a matter of trying your best, so that's another thing to keep in mind.

And also, try your best not to over promise security. In this day and age in particular, it's just getting, unfortunately a matter of when, not if, something bad would happen with data so you want to avoid that by not over promising things when you can.

Nick: And on the other side of the spectrum for consumers, gamers and esports competitors, you know, kind of similar to what we talk about in our podcast episode on cybersecurity, you always want to practice safe cyber hygiene. And part of that involves knowing what data you're giving up and not being afraid to push back or try to research more if necessary. It's always a good idea to use a password manager to change up your usernames and passwords so you don't use the same one on every site and so you can also pick a very strong password that's unlikely to get determined by somebody else. You can also use two-factor authentication to minimize the impact of any breaches that occur.

And at the end of the day it's all about consumer choice and being an educated consumer. So read up and understand what's going on. And as terrible as this sounds, take the time to read the privacy policies and the terms of service that come with your games, don't just click accept like most people do. And feel free to reach out to the game developer if you have questions, who knows, they may be happy to talk with you about this issue. But as always, the best idea is to work with an attorney who understands the industry and the legal trends that are at play in this fast-changing landscape.

Steve: Agreed 100%, Nick. That's all we have today on data privacy in gaming, that's pretty exciting stuff. Unless you have anything further to add, Nick.

Nick: That's all I've got, just make sure to be on the lookout for other episodes of LAN Party Lawyers Podcast and until then...

Steve: Game on.

Nick: ...game on.

Carlton Fields publications should not be construed as legal advice on any specific facts or circumstances. The contents are intended for general information and educational purposes only, and should not be relied on as if it were advice about a particular fact situation. The distribution of this publication is not intended to create, and receipt of it does not constitute, an attorney-client relationship with Carlton Fields. This publication may not be quoted or referred to in any other publication or proceeding without the prior written consent of the firm, to be given or withheld at our discretion. To request reprint permission for any of our publications, please use our Contact Us form via the link below. The views set forth herein are the personal views of the author and do not necessarily reflect those of the firm. This site may contain hypertext links to information created and maintained by other entities. Carlton Fields does not control or guarantee the accuracy or completeness of this outside information, nor is the inclusion of a link to be intended as an endorsement of those outside sites.