U.S. Department of Justice
Office of Justice Programs
Bureau of Justice Assistance

Transcript: Innovations in Justice—Real Crimes in Virtual Worlds: An Interview With Dr. Brian Regli and Dr. Robert D'Ovidio

The Bureau of Justice Assistance (BJA) Justice Podcast Series is designed to provide the latest information in justice innovations, practices, and perspectives from the field of criminal justice. In this edition, Cornelia Sigworth, BJA Policy Advisor, interviews Dr. Brian Regli, Chief Executive Officer of Drakontas LLC, and Dr. Robert D'Ovidio, Associate Professor at Drexel University, about crime in virtual worlds and online gaming communities.

Cornelia Sigworth: Hello, this is Cornelia Sigworth. I'm a Policy Advisor with the Bureau of Justice Assistance. Today I am sitting down with Dr. Brian Regli from Drakontas Communication Tool and Dr. Robert D'Ovidio from Drexel University. Dr. Regli is the Chief Executive Officer of Drakontas Incorporated [LLC, www.drakontas.com]. In this role, he is responsible for developing product commercialization strategies for emerging technologies. Dr. D'Ovidio is an Associate Professor at Drexel University, where he teaches for the Criminal Justice Program and directs Drexel's research program in computer crime and digital forensics. Both Dr. Regli and Dr. D'Ovidio are working with the Bureau of Justice Assistance to develop curriculum materials to increase awareness of crimes committed in virtual worlds and to build capacity among state and local law enforcement [agencies] to combat these crimes.

So, Brian, when you think of video games, you think of fun, not crime. How are people exploiting virtual worlds and online video game worlds for criminal purposes?

Dr. Brian Regli: Online video games are all about building communities. They're about multiplayer games—you can play things alone, sort of, sit there and play Solitaire alone, you can play Angry Birds alone, but generally speaking, these [online] games are built to bring these communities together. So you have certain goals that you want to achieve. [In] FarmVille, you want to get your products to market, you've lost your sheep. [In] World of Warcraft, you've got to kill an ogre, you have to destroy the dragon's lair. So to accomplish those goals, you bring together groups of people. And it's that social experience that's fundamental to these online games, and that social experience then drives your ability to achieve those goals. And your objectives then flow from what that community brings to you.

Obviously, from the gaming company's perspective, the more people you bring into the community, the more valuable the game is, the more money they are going to make, so all of the incentives within the game are built to create those communities and get you to basically participate and invest in that community. The problem of course is that any time you build a great amusement park or a great neighborhood park, it's going to bring millions of people; everybody is going to want to come.

So there are good people who show up with good intentions, [and] there are bad people that will show up with bad intentions. And those that show up with criminal intent are going to look at how the playground is built. They are going to look at how to exploit the way the playground is built; they are going to look for the dark corner to lurk in. They are going to look for the child that might be on the edge of the playground who might be playing alone. And the same sorts of environments exist in the virtual communities as well, where you can pick people off, socially engineer a circumstance. And maybe [there is] a person who has an intention to find a 13-year old girl [and] who's posing as a 13-year old girl because that's the avatar they created, that's the virtual instantiation of themselves that they created. Now they can convince that person maybe to get together on a play date at a real park, and all of a sudden you have an online enticement case. Or maybe it is a group of criminals who have to figure out where the drug drop is going to be tonight or to figure out, frankly, when they are going to kill the person in the gang that they are opposed to. And they will be able to use some of the chat features of these games, [or] they'll be able to use some of the file transfer and sharing features of these games, so they can coordinate and they can collaborate on a channel that maybe law enforcement is not necessarily listening to or paying attention to.

So ultimately the games are fun, and the games are built to be social. But the tools that are used to create these social games are the same tools that can be used to exploit children; they're the same tools that can be used to coordinate crime. And the gaming companies didn't build them to coordinate crime or exploit children; they built them to be fun, but it's really two sides of the same coin in terms of the actual consequences of how these games are being used by the criminals.

Cornelia Sigworth: Rob, what makes virtual worlds and online video game worlds attractive targets for criminals?

Dr. Robert D'Ovidio: Well, as Brian mentioned, there are a lot of people there. So in some of these worlds there are 100 million+ users that have signed up; doesn't mean that there are 100 million+ active players, but people that have signed up and have gotten accounts. So there are plenty of targets to victimize. I think there are a number of attributes of the games that also are attractive to criminals. The communications capabilities, for instance, somebody—the ability to go in and to use various types of chat interaction, whether it's text chat, whether it's in a formal chat room or an instant messaging environment, whether it's voice chat or video chat. These environments or these capabilities provide ways to interact with people, whether it is an offender interacting with a potential victim for sexual exploitation, whether it's two offenders that are using the Xbox Live environment to orchestrate a criminal activity if they are involved in a gang or involved in a terrorist organization. These communication capabilities are very attractive in that law enforcement [officers] have not traditionally looked at them as sources for criminal communication, so they're not monitoring these channels.

Cornelia Sigworth: So, that sounds like it gets at what may be perhaps one of the biggest challenges facing the law enforcement community when it comes to addressing crime in the virtual worlds and online video game worlds. Can you speak a little bit more about those challenges?

Dr. Robert D'Ovidio: Yes, so there are a number of challenges. One is the fact that these places are new. When it comes to the online gaming world, it is a relatively new phenomenon, so law enforcement [officers] aren't familiar with the capabilities within these spaces. They are not familiar with the economics of these communities to understand that they're ripe environments for identity theft, they're ripe environments for money laundering. You have the abilities to go and steal virtual goods, which hold real-world value, and you have the ability to transfer funds from those virtual worlds into the physical worlds. So awareness is one problem.

On a more technical level, we see the means to access these worlds at times involve video game consoles: the PlayStation 3, the Xbox 360, the Nintendo Wii, and the equivalent hand-held devices. But we don't have the forensics tools available for these gaming consoles as we have for traditional PCs, for laptops, [and] cell phones. And that creates a forensic challenge for the law enforcement community. So there needs to be alternatives, alternative methodologies developed for these consoles; as well, there needs to be research and development in the area of tools for these consoles.

Cornelia Sigworth: And Brian, can you tell us a little bit more about the economic crime that can occur in these virtual worlds and perhaps what law enforcement [officers] should be looking for in that regard?

Dr. Brian Regli: So almost all of these games have an economy associated with them. They have virtual currencies, there are ways to use real-world currencies to buy virtual currencies, [and] you can earn virtual currencies by playing the game. And then there are objects in the game that are valuable to the people who play the game. So we're not talking about significant money in most cases; you're not talking about more than a couple of cents here and a couple cents there for these little virtual goods. But in some cases it is much more than a micropayment. There are games in which you have objects that are worth hundreds of thousands of dollars, and not just because the game says they're worth hundreds of thousands of dollars, but because there are real-world web sites, there are real-world exchanges where you can actually buy and sell these goods and services. So within the context of game play, especially in games that incent entrepreneurial activity, there is a whole economic framework that comes with playing the game.

So what kinds of crimes exist within those games are the kinds of crimes that you would find committed with bank fraud, committed with wire fraud, [and] committed with theft of goods; because anything that you can buy and sell in the real world, you can buy and sell in the virtual world. And any kind of transaction, currency transaction, transactions for goods and services, [and] loans, those can exist in the virtual worlds as well. So the kinds of crimes that we've seen, everything from money laundering to theft of goods and services, to basically phishing [and] spear-phishing, the kinds of cyber attacks you would find that are usually oriented towards a bank account, are now actually being oriented towards your World of Warcraft account. So a lot of the games that are very popular, well, they're generating huge profits, they're generating huge amounts of money, and people are attacking where the money is. So that's the sort of economic crimes we've been seeing in this space.

Cornelia Sigworth: So you say that you can buy or sell anything in the virtual world that you could buy or sell in the real world. Is it also fair to say then that you could steal anything in the virtual world that you could steal in the real world?

Dr. Brian Regli: It depends on the game. Some games are more susceptible than others, but generally speaking, yes. There are certain games that actually promote theft and piracy and stealing as part of the game play.

So there's some real questions in the law enforcement [community] as to whether or not theft in a game that is meant to be protecting the individual players, protecting their assets, is the same as theft in a game in which, again, theft is built into the game play. The whole concept of virtual-world property rights and intellectual property associated with those property rights is also something that is being debated in a variety of law enforcement jurisdictions throughout the world. There are places like the Netherlands in Europe and South Korea where they are actively prosecuting individuals who have stolen virtual goods from a game or [where] a child has basically lost an object and the person who has stolen that object has been convicted and basically forced to pay restitution and damages. So there are real cases out there in the world; less so in the United States, but certainly on a global basis. And that's in great part because the gaming companies and law enforcement [agencies] are beginning to understand that the money that you have in your virtual account for World of Warcraft gold is potentially as valuable as the money you have in your bank account. And that's the kind of response that we are beginning to see [that] law

enforcement needs to make or should be making. And to get geared up for that is a real challenge because it's new and it's different.

Cornelia Sigworth: And so facing that challenge, what role can the industry play in sort of assisting law enforcement or helping to prevent some of this criminal activity?

Dr. Brian Regli: Well, I think what the industry needs to do, besides continuing to police its own games as they are actively doing, is to communicate more with law enforcement and to do the best that they can to help educate law enforcement as to the nature of the game play and the kinds of resources that they have available for law enforcement should an investigation be required. Now there are many companies that have worked very hard to build law enforcement guides, to build the kind of information repositories that law enforcement can use; and in those areas, clearly there is a lot of value that the companies see in investing in giving that information to law enforcement. So the more that they can educate law enforcement about what they have available in the case of an investigation, the more law enforcement is likely to be able to ask productive questions. Because ultimately, for a gaming company, it's a cost when somebody calls the general counsel and issues a subpoena for information about a subscriber. There's a cost in generating that information, but if we can sort of create a better relationship between law enforcement and the industry and more of a common knowledge of the objectives of both sides, what [the] industry is going to get out of it is better intellectual property protection, they're going to get a happier customer base, and they're going to be able to over time make sure that their community, their neighborhood, their playgrounds so to speak, is as safe as it really was designed to be originally. So that's the goal.

Cornelia Sigworth: And, Rob, given that this is a new crime, at least—maybe not a new crime but in a new arena—are there gaps in federal and state legislation when it comes to having the proper legal tools to arrest and prosecute people who commit crime in these environments?

Dr. Robert D'Ovidio: Well, I think there are and there aren't. When you talk about crimes—recently hundreds of thousands of World of Warcraft account credentials were stolen, so that's nothing more than an identity theft-related, identity theft case, which we've seen time and time again. And the means by which [some]one stole those accounts were a network intrusions, so we have federal law and equivalent state law to address network intrusions where the individual goes in and steals or copies data. So we are on firm ground there. We do have a strong body of case law to help guide law enforcement in what's correct and what's not correct in dealing with those types of investigations and in prosecuting those types of crimes.

Where I think things become a little less clear is when we are talking about the theft of virtual goods. And it's not so much that we don't have statutes to address theft, it's that we have to start convincing the law enforcement community, and more importantly the prosecutors and judges, that the theft of a virtual sword from World of Warcraft is a theft. And I think once we start looking at that intellectual property as—recognizing that it holds real-world value, then we can start to apply more traditional statutes that have been used to prosecute the theft of traditional products, or even the theft of other digital products when it comes to music downloads or movies.

We still have a long way to go and it's not an easy process. What we found through this training program is that there are mixed opinions in terms of whether these are actually crimes. And we talk about the cases that, as Brian mentioned earlier, that have existed in European countries and in South Korea, but really none have taken place here in the United States yet, so we don't have a body of case law to look at to give us guidance on how to move forward with these types of cases.

Cornelia Sigworth: And every time we have this discussion and people learn of this, the question always comes up about what parents can do to safeguard their children who play online video games and play in virtual worlds. Obviously there is fear of predation, there's fear of economic fraud and stealing identities of the players and easily tricking children. Can you speak to that a little bit, Brian?

Dr. Brian Regli: Sure, and I think Rob should speak to it a little bit as well. I have a sixth grade son and a fourth grade daughter. And I'm a gamer. I play a lot of games, they play a lot of games, [and] we play games together. And yeah, I do get a little bit scared, especially of my son and my daughter because as they get more knowledge they are more likely to explore in the world and find things that are inappropriate. I am already beginning to see that in both cases. So that's not unusual for a child to explore.

The issue is for the parent to be aware of the playground—to know that this is the sort of thing that you do in those playgrounds [and] here are the other people who are playing in this playground—and then help their child identify the patterns; help their child understand certain things that are inappropriate in these particular communities. And so some of that requires you sitting down and playing the game as a parent, or at least sitting while your child plays the game, and beginning to sort of build that relationship of trust with them, so they know [that] if something inappropriate is going on or if something they perceive is inappropriate, they are still willing to come to you and sort of share and explain that to you. And that's a combination of good parenting, but it is also doing your research and understanding what's going on.

So the extent to which there are resources that the federal government and other agencies can provide to help educate parents, I think that is really critical because most parents don't even know what their kids are doing on their Xbox. I happen to [know] because I enjoy playing and I kind of get a kick out of it too, and so I am naturally drawn to understanding these things, but most parents aren't. So I think what parents need to do is invest time and understanding their child's interest and be willing to kind of take that technical leap to sort of get into these games a little bit and see what they are about. And 99.9 percent of what happens in these games are fun, they're social, they're great. You know, I think in many ways they are tremendous evolutions in how we entertain ourselves and how we solve problems and how we learn how to work together in a community. There's a lot of great things that come out of

games. But ultimately, I think those are the kinds of things that a parent needs to be doing.

Dr. Robert D'Ovidio: Yeah, I think that awareness is very, very important. And as Brian mentioned, there's a time commitment that parent's have to make in understanding the vulnerabilities within specific gaming environments and within specific virtual worlds. And you are not just going to drop your child off at a [real-world] park in the physical space without knowing the environment, without feeling comfortable that the environment is safe. Why should you do that in the virtual world when you know that the PlayStation 3, the Xbox 360, [and] the Wii all have these communicative capabilities that allow people to play with other people all over the world? So it's just [that] the onus is on the parent to understand the environment that their kids are in.

The other thing too is that they [parents] have to be very vigilant with this in that it's one—just because they're playing one game today and there are certain capabilities in one game—[with] the new game that comes out tomorrow, there might be additional capabilities, so it's not something that you do on a—it's not a "one shot and done" type of thing; you need to be very, very on top of things.

But I also think that it is important to have an open dialogue with your child. You know, you can be familiar with the capabilities, but as we talk about in more traditional types of virtual environments, whether its Facebook or Myspace, or using chat rooms or instant messaging and texting capabilities, you need to set firm rules and make sure you check up on your children that they're following the rules. The other thing too is there are certain—the PlayStation 3 has that capability of child protection capabilities built in. You can download a piece of software by one of the antivirus companies, I believe it's Trend Micro, that does provide that child protection, those child protection features that are similar to what's available for traditional computers, so it will block out sexually oriented texting and chat conversations.

There are certain virtual worlds that children can play where you can limit those chat and interactive capabilities and you can limit it by cutting it all off or you can limit it to only allow for the communication and the receiving of communication that's predefined by the game provider or the virtual-world provider. So that ensures that there's not going to be any sexually graphic communication or violent communication that's being exchanged.

But again, as Brian mentioned, it all comes down to understanding the environment that your kids are in. And I can't stress enough that this is not a problem that the law enforcement and the criminal justice community can handle by itself. The parents are part of that community when it comes to responsibilities of keeping their own children safe, and so they need to play their part. And hopefully in doing so they prevent crime from even happening to begin with.

Cornelia Sigworth: Well, thank you both very much for your time today. It's [a] very interesting interview, and we look forward to talking to you again soon.

Dr. Brian Regli: Well, thank you.

Dr. Robert D'Ovidio: Thank you.

Closing: Thank you for taking the time to join us for this conversation. If you found the discussion interesting, we encourage you to visit the BJA web site for more innovative ideas and best practices at www.ojp.gov/BJA.

From all of us here at BJA, thank you for tuning in to today's podcast. We hope you will join us again for another edition of BJA's Justice Podcast Series.

CONTACT US

Bureau of Justice Assistance
Office of Justice Programs
810 Seventh Street NW.
Washington, DC 20531
Phone: 202–616–6500
Toll free: 1–866–859–2687
E-mail: AskBJA@usdoj.gov
Web site: www.ojp.gov/BJA