PLAYING IN THE DARK: HOW ONLINE GAMES PROVIDE SHELTER FOR CRIMINAL ORGANIZATIONS IN THE SURVEILLANCE AGE

Matthew S. Ruskin*

TABLE OF CONTENTS

I. INTRODUCTION

The 2010 dark comedy "Four Lions" follows an inept British terrorist cell determined to conduct an attack that will "echo through the ages."[1] Hijinks follow. Among the hilariously misguided techniques the gang of terrorists uses to subvert various anti-terrorist intelligence agencies is its use of a fictional children's online game called "Puffin Party."[2] There, members of the gang use their puffin avatars to communicate with each other while presumably out of law enforcement's earshot.[3] In one scene, Omar, the smartest of the group, reports a

* J.D. Candidate, University of Arizona James E. Rogers College of Law, Class of 2015; Senior Managing Editor at the *Arizona Journal of International & Comparative Law*. Special thanks to everyone who helped throughout the process of preparing this Note, to the Journal, to my family, and to my fiancée, Heidi Nielson.

1 FOUR LIONS (Film4 Productions 2010).

2 *Id.*

3 *Id.*

conversation with his emir,[4] saying his "puffin has communicated with [the emir's] puffin," who has ordered them to make some bombs.[5]

While this waggish, albeit dark, scene may seem implausible, its real-life manifestation is more fact than fiction. Recently released law enforcement documents report that criminal organizations have started using the communication features available in online games to conduct business.[6] Gangs like the Bloods and the Mara Salvatrucha[7] reportedly use chat features available in online gaming platforms like Xbox Live to recruit members, organize business, and even order hits.[8] Other organizations use in-game chat features to organize drug smuggling rings.[9] Such activity makes criminal communication both easier to conduct and more difficult to detect.

In fact, both British and American agencies have identified games and virtual environments, which they term "GVEs," as havens for illegal activity.[10] Recently released documents show that, because of fears that "criminal networks could use the games to communicate secretly, move money or plot attacks," intelligence operatives have entered the video game terrain as virtual spies.[11] While there, the spies create "make-believe characters to snoop," "recruit informers," and collect "data and contents of communications between players," because features common to video games, such as "fake identities," and "voice and text chats" provide an ideal place for criminal organizations to operate.[12] A 2008 document released by the National Security Agency (NSA)[13] warned that, although "[o]nline games might seem innocuous . . . they ha[ve] the potential to

---

[4] An emir is a military commander. *Emir*, ENCYCLOPEDIA BRITANNICA, http://www.britannica.com/EBchecked/topic/185879/emir (last visited July 24, 2014).

[5] FOUR LIONS, *supra* note 1.

[6] *Federal Bureau of Investigation Situational Information: Bronx Members Communicating Through Playstation Network,* FBI, (May 25, 2011), http://info.publicintelligence.net/FBI-BloodsPSN.pdf; *NJ Common Operating Procedure: MS-13 Using Gaming Consoles to Conduct Business*, N.J. REG'L OPERATIONS INTELLIGENCE CTR., (Sept. 21, 2010) [hereinafter *MS-13 Using Gaming Consoles*], http://info.publicintelligence.net/NJROIC-GangConsoles.pdf.

[7] Also known as MS-13, this gang of predominantly Salvadorian members originated in Los Angeles in the 1980s, and likely consists of tens of thousands of members in the United States and Central America. *Mara Salvatrucha 13 (MS-13)*, GANGS.ORG, http://gangs.umd.edu/Gangs/MS13.aspx (last visited July 15, 2014).

[8] *MS-13 Using Gaming Consoles, supra* note 6, at 1.

[9] Jared Savage, *Crims Plan Using Gaming Consoles*, N.Z. HERALD (Feb. 23, 2013), http://www.nzherald.co.nz/nz/news/article.cfm?c_id=1&objectid=10867137.

[10] Mark Mazzetti & Justin Elliott, *Spies Infiltrate a Fantasy Realm of Online Games*, N.Y. TIMES, Dec. 9, 2013, at A1, *available at* http://www.nytimes.com/2013/12/10/world/spies-dragnet-reaches-a-playing-field-of-elves-and-trolls.html.

[11] *Id.*

[12] *Id.*

[13] While this Note focuses primarily on criminal intelligence gathering rather than on counterterrorism and national security, many of the issues it discusses relate to both.

be a 'target-rich communication network' allowing intelligence suspects 'a way to hide in plain sight.'"[14]

Furthermore, according to the NSA, "Massively Multiplayer Online Games (MMOG) are ideal locations" for criminals "because of the enormous scale on which they are played," featuring thousands of subscribers simultaneously using various servers hosted in a wide array of places, including on gamers' own dedicated servers.[15] Additionally, GVEs may often be accessed "via mobile devices connected wirelessly," such as phones, handhelds, or laptops.[16] Through connections to online gaming environments, these types of devices allow for an additional place where users can interact, connect, or share.[17] These sites can be "advertised" in online games and password-protected so that they function essentially as private meeting places for criminal organizations.[18]

Consequently, the online gaming landscape poses a unique challenge for law enforcement because it not only involves a new realm wherein criminal organizations thrive, but it also represents communications that more closely involve innocent parties and are more technically difficult to intercept. As a result, law enforcement around the world will need to make difficult decisions regarding surveillance and regulation of these types of communications.

The technical difficulties posed by in-game communications raise an especially difficult dilemma for law enforcement because they present issues in an area skirting the edge of law enforcement's technological ability. Often times, even if law enforcement agencies have the legal authority to conduct surveillance, they do not have the technical capability to survey the use of communications like those that take place in online games.[19] The Federal Bureau of Investigation (FBI) labels this difficulty the "going dark" problem, which explains how intelligence-gathering officials lack the technological ability to carry out intelligence gathering as quickly as required.[20] That problem manifests itself as an inability for prosecutors to effectively track and counteract criminal behavior on large scales, as was the case in 2009, when the Drug Enforcement Agency learned of an international drug and weapons smuggling ring with operations in North and South America, Europe, and Africa.[21] Because the leader of that ring knew which

---

[14] Mazzetti & Elliot, *supra* note 10.

[15] *NSA Files: Games and Virtual Environments Paper*, GUARDIAN (Dec. 9, 2013) [hereinafter *GVE Paper*], http://www.theguardian.com/world/interactive/2013/dec/09/nsa-files-games-virtual-environments-paper-pdf.

[16] *Id.*

[17] *Id.*

[18] *Id.*

[19] *Going Dark: Lawful Electronic Surveillance in the Face of New Technologies: Hearing Before the Subcomm. on Crime, Terrorism, and Homeland Security of the H. Comm. on the Judiciary*, 112th Cong. 2 (2011) [hereinafter *Going Dark*] (statement of Valerie Caproni, General Counsel, FBI), *available at* http://www.fbi.gov/news/testimony/going-dark-lawful-electronic-surveillance-in-the-face-of-new-technologies.

[20] *Id.* at 2.

[21] *Id.*

communications lacked "intercept solutions," much of the ring still functions today.[22] The primary difficulty in prosecuting crimes like these relates to law enforcement's desire to access data in real or near-real time, rather than to access stored information.[23]

In the wake of these interests, how governments approach the regulation and surveillance of online games will greatly affect their citizens and a broad swath of the business world. The video game industry in the United States alone generates forty billion dollars of revenue and employs over 170,000 people in over 29,000 businesses.[24] Examining how law enforcement can effectively monitor and combat organized criminal activity that involves the use of online games, this Note assesses the technical feasibility of tracking communications in online games along with the legality and the efficacy of doing so. The Note begins with an overview of the new issues that arise from the proliferation of online gaming. From there, it summarizes both past and present legal structures that various countries have used to address related criminal activity. Next, this Note discusses the legal issues provoked by regulation and surveillance of online games. Finally, it examines the possible steps that governments can take in the future to find the appropriate balance between effective prosecution and the interests of liberty, innovation, and cost-effectiveness. This Note ultimately argues that, although the potential for criminal use of online games is too great for law enforcement agencies not to monitor, the best approach will be a limited one that allows individual companies to structure their communications systems and moderate their users most efficiently.

II. LEGAL OVERVIEW

A. New Problems Created by Gaming Communication

The intelligence community was quick to identify the type of services that criminal groups might use to do business. A 2008 document from the NSA explained known operational uses of "feature-rich Internet communications" technology among criminal groups, such as "email, VoIP,[25] chat, proxies, and web forums."[26] The NSA also noted a high likelihood that criminal groups would make "wide use of the many communications features offered by Games and Virtual Environments."[27] Because, at that point, agencies like the NSA could not

---

22 *Id.*

23 *Id.*

24 *Video Games in the US: Market Research Report*, IBISWORLD, http://www.ibisworld.com/industry/retail.aspx?indid=2003&chid=1 (last visited Mar. 2014).

25 "Voice over Internet Protocol"

26 *GVE Paper, supra* note 15.

27 *Id.*

even "recognize the traffic" and were therefore unable to "determine how targets [were] using the communications features of GVEs," the NSA argued that intelligence operations needed "to begin taking action now to plan for collection, processing, presentation, and analysis of these communications."[28]

Online games were particularly troublesome for intelligence-gathering agencies because of the games' ability to "allow individuals to gather with like-minded others online" and chat via text or voice over "private chat (P2P), group chat, chat to an alias, and broadcast chat."[29] Additionally, GVEs are particularly likely to use "convergent technologies."[30] For example, Xbox Live can be run via a gaming console or "connect[ed] via a PC to normal MSN chat."[31] Similarly, the virtual world Second Life "offers the ability to anonymously text to a . . . phone" or to place "anonymous voice calls" that do not disclose phone numbers to either party or "show up in collection."[32]

On a broader scale, both intelligence and criminal organizations recognize that games provide "attractive communications channels" because "in-game conversations often are difficult or impossible to monitor."[33] Additionally, most games contain "capabilities like VoIP, chat, and file transfers that allow real-time communications to take place," and much of that traffic is not logged in the same way as traditional Internet traffic.[34] Moreover, in-game communications are not subject to current "Internet control methods" because such communications feature speech and text that mingle with data from games.[35] This results in the increased possibility that "authorities will overlook communications they would normally prohibit."[36]

Communication that takes place in online games poses a unique challenge for law enforcement for two reasons. First, it exists outside the scope of traditional evidence gathering techniques because it takes advantage of VoIP technology. Unlike traditional communication, which involves transmitting analog voice signals over wires, VoIP converts a voice signal into digital information before transporting it in packet form to its destination, where the information is then converted back into an audio signal. Because VoIP is relatively new, both intercept technology and law enforcement procedures have not developed effective strategies for monitoring its use.

Second, online gaming communication poses a distinctive problem for law enforcement because of the way it is organized. In traditional forms of

---

28 *Id.*

29 *Id.*

30 *Id.*

31 *GVE Paper*, *supra* note 15.

32 *Id.*

33 *Infiltrating a Virtual Gaming World*, N.Y. TIMES (Dec. 10, 2013), http://www.nytimes.com/interactive/2013/12/10/us/politics/games-docs.html?ref=world.

34 *Id.*

35 *Id.*

36 *Id.*

communication, two parties who likely know each other take part in two-way conversation. However, in online games, large groups of individuals—most of them strangers—engage in communication without a discernible end-point. Therefore, criminal organizations are capable of using online chat features among innocent parties. Often times, it is difficult, if not impossible, to separate criminal communications from the other communications taking place in the group.

This type of organization lends itself to three more issues. First, the Internet provides anonymity, which in turn gives users of this method of communication the ability to experiment with illicit activities. Before the Internet, criminal organizations relied on "underground networks where personal connections were essential to consumers looking to obtain illegal products."[37] But the Internet now allows criminal organizations to conduct business in public, and members of the public can anonymously access illegal information.[38] Additionally, those who might previously have refrained from engaging in criminal activity for fear of revealing their identities now enjoy safer access to illegal information.[39] Given these issues and the proclivity of anonymous Internet users to engage in other unsavory, and often hateful, activity, the presence of organized crime on the Internet raises the question of whether the benefits of online anonymity outweigh the harmful effects.

Second, criminal organizations now communicate more easily because of the Internet.[40] The expansion of the Internet has coincided with the development of new media through which parties can exchange information. The practice of branching out into online games demonstrates one of the more clever applications of communications technology that criminal organizations have developed. And its use, especially in conjunction with other forms of communication, allows members of criminal organizations more variety, and often more security, to communicate, strategize, and carry out organizational activities.

Finally, the Internet provides criminal organizations with a unique medium for advertisement.[41] For one, online games give criminal organizations access to a public audience for solicitation and promotion. They also provide an audience from which organizations can recruit and teach members.[42] Most alarmingly, however, criminal organizations may increasingly use online games to

---

[37] Kendall Vitale, *Barricading the Information Superhighway to Stop the Flow of Traffic: Why International Regulation of the Internet Is Necessary to Prevent Sex Trafficking*, 27 AM. U. INT'L. L. REV. 91, 106-07 (2012).

[38] *Id.*

[39] *Id.*

[40] *Id.*

[41] *Id.*; *see also* MS-13 USING GAMING CONSOLES, *supra* note 6.

[42] This practice may even extend to terrorist organizations. Chris Gourlay & Abul Taher, *Virtual Jihad Hits Second Life Website*, SUNDAY TIMES (Aug. 5, 2007), http://www.thesundaytimes.co.uk/sto/news/world_news/article69229.ece.

seek out victims.[43] As a result of these nuances, fighting crime online presents new challenges for law enforcement agencies.

B. Law Enforcement's Response

1. United States

In the United States, the federal government's authority to conduct court-ordered communications surveillance comes from Title III of the Omnibus Crime Control and Safe Streets Act of 1968 and the Foreign Intelligence Surveillance Act of 1978 (FISA).[44] However, these acts did not allow for effective surveillance of digital communication.[45] In order to address that problem, Congress enacted the Communications Assistance for Law Enforcement Act (CALEA) in 1994.[46] CALEA requires telecommunications carriers to develop "intercept solutions in their networks to ensure that the government is able to intercept electronic communications when lawfully authorized."[47] In response to the changing telecommunications field, CALEA has been expanded to include VoIP communications, but only to the extent that such communications take place through services that are "fully inter-connected with the public switched telephone network."[48] However, the modern communications landscape still poses a number of problems for the application of CALEA.

Most importantly, a large portion of popular Internet-based communications does not fall under CALEA's purview.[49] CALEA does not cover the majority of VoIP communications.[50] Further, increasingly complex communications techniques often use an array of modalities at the same time, and any of them may fall outside of CALEA's authority.[51] In addition, because CALEA relies on the communications providers themselves to come up with solutions, and because it only requires providers to meet certain industry standards, the compliance measures that providers take often fail to provide law enforcement with sufficient tools for gathering evidence.[52]

With these problems in mind, the federal government has adopted several measures to increase its crime-fighting ability. First, it established the Domestic

---

43 Vitale, *supra* note 37, at 107.
44 *Going Dark*, *supra* note 19, at 3.
45 *Id.*
46 *Id.* at 4.
47 *Id.*
48 *Id.*
49 *Going Dark*, *supra* note 19, at 4.
50 *Id.*
51 *Id.*
52 *Id.* at 6.

Communications Assistance Center (DCAC).[53] The purpose of the DCAC is to "leverage the research and development efforts of Federal, State, and local law enforcement with respect to electronic surveillance capabilities, facilitate the sharing of technology between law enforcement agencies, advance initiatives to implement solutions complying with CALEA, and seek to build more effective relations with the communications industry."[54] Given both the DCAC's vague purpose statement and the secrecy surrounding its implementation, it is unclear exactly what the DCAC does.[55]

Second, while not yet implemented, Congress is considering another expansion of CALEA that would include stricter guidelines for communications providers and cover a wider range of Internet communications.[56] The proposed expansion would likely mandate that (a) "communications services that encrypt messages have a way to unscramble them"; (b) "foreign-based providers that do business inside the United States install a domestic office capable of performing intercepts"; and (c) "developers of software that enables peer-to-peer communication redesign their service to allow interception."[57]

2. Surveillance Abroad

Other countries have taken similar steps. In the United Kingdom, for example, the Government Communications Headquarters (the U.K.'s spy agency, which is also known as the "GCHQ") has been broadly monitoring Internet use since 2008.[58] Additionally, in 2006, it launched the Serious Organized Crime Agency (which has been replaced by the National Crime Agency) to combat, in a large part, organized crime on the Internet.[59] Those programs allow British intelligence agencies to intercept communications through "data interceptors" placed on fiber optic cables.[60] Increasingly, however, the U.K. intelligence community has found that, as is the case in the United States, the use of VoIP technology is eroding law enforcement's ability to conduct adequate

---

[53] Declan McCullagh, *FBI Quietly Forms Secretive Net-Surveillance Unit*, CNET NEWS (May 22, 2012), http://news.cnet.com/8301-1009_3-57439734-83/fbi-quietly-forms-secretive-net-surveillance-unit/.

[54] *Going Dark*, *supra* note 19, at 7.

[55] McCullagh, *supra* note 53.

[56] Charlie Savage, *U.S. Tries to Make It Easier to Wiretap the Internet*, N.Y. TIMES, Sept. 27, 2010, at A1, *available at* http://www.nytimes.com/2010/09/27/us/27wiretap.html.

[57] *Id.*

[58] Kadhim Shubber, *A Simple Guide to GCHQ's Internet Surveillance Programme Tempora*, WIRED (June 24, 2013), http://www.wired.co.uk/news/archive/2013-06/24/gchq-tempora-101.

[59] *See About the NCA*, NAT'L CRIME AGENCY, http://www.nationalcrimeagency.gov.uk/ (last visited Aug. 22, 2014).

[60] Shubber, *supra* note 58.

surveillance.[61] Because "internet calls are virtually impossible to listen in on" without the use of a bug installed on the computers sending or receiving the calls, the GCHQ has started "working on ways to get around the problems caused by this use of the internet."[62] Such methods include reportedly requiring Internet companies both to keep records of all messages sent on their networks and to install "Deep Packet Inspection equipment."[63]

Even so, the United Kingdom contends that it balances its surveillance with privacy and that it regulates surveillance to ensure its effectiveness. According to its Parliament's official website, "[p]rivacy and proportionality are the praetorian guards that stand in the way of unfettered surveillance."[64] Presumably with this in mind, Parliament enacted the Data Protection Act, which "attaches the most careful attention" to "'sensitive' personal data," such as political beliefs, union activism, religious beliefs, and health and sexual history.[65] The trick, according to Parliament, is to balance the protections afforded to innocent citizens and even "minor infringers," like "the pensioner whose dog fouls the local park," with more serious offenders, like terrorists, serious criminals, and fraudsters, who have something to hide.[66] For the first category, privacy should be at a premium; however, for the second, the United Kingdom argues that most "would want few stones unturned to bring such people to justice."[67]

With such a policy in mind, the Regulation of Investigatory Powers Act 2000 (RIPA) "controls . . . covert surveillance."[68] Parliament enacted it to function alongside "associated secondary legislation and codes of practice," and to provide a "framework designed to ensure that public authorities comply with the European Convention on Human Rights."[69] In doing so, Parliament aimed to address concerns about the perceived low threshold for surveillance powers, unreliability, and misuse of investigatory powers.[70] RIPA subjects public

---

[61] Jason Lewis, *GCHQ Warns It Is Losing Terrorists on the Internet*, TELEGRAPH (Apr. 8, 2012), http://www.telegraph.co.uk/news/uknews/terrorism-in-the-uk/9192209/GCHQ-warns-it-is-losing-terrorists-on-the-internet.html.

[62] *Id.*

[63] *Id.* Deep Packet Inspection involves scanning each packet that passes through a network and then either blocking it or routing the packet to its appropriate destination. Alex Wawro, *What Is Deep Packet Inspection?*, PCWORLD (Feb. 1, 2012), http://www.pcworld.com/article/249137/what_is_deep_packet_inspection_.html. This process can be used to gather a person's personal information, like "age, location, and shopping records." *Id.*

[64] Grahame Danby, *Surveillance in Society*, *in* KEY ISSUES FOR THE NEW PARLIAMENT 2010 86, 86 (2010), *available at* http://www.parliament.uk/documents/commons/lib/research/key_issues/Full-doc.pdf.

[65] *Id*.

[66] *Id.*

[67] *Id.*

[68] *Id.*

[69] Danby, *supra* note 64, at 86.

[70] *Id.*

authorities, including those at a local level, to regulations that control their access to communications data.[71] It aims to control how law enforcement accesses non-content communications data.[72] This data, usually stored by communications providers for billing purposes, includes information like dialed phone numbers.[73] Under RIPA, government bodies must provide specific reasons for accessing information, such as crime prevention, and the agencies must also comply with established rules.[74]

Moreover, the United Kingdom seeks to design its surveillance practices to keep up with changing technology. Accordingly, the United Kingdom's Interception Modernisation Programme aims to keep pace with technology "to extend further the type of data that has to be retained," including "interactions in chat rooms and social networking sites."[75] However, such programs have raised outcry over privacy concerns. For example, the United Kingdom abandoned a recent proposal to store communications in a centralized government database as a result of concerns over privacy.[76] It is now considering a substitute proposal that would impose requirements on Internet service providers (ISPs) "to keep extra data in a way that would make it easily accessible" to law enforcement agencies.[77] Such a program would likely be the functional equivalent of CALEA in the United States.

The United Kingdom has also started branching out into the virtual realm. According to government documents, by the end of 2008 GCHQ had set up what it called its "first operational deployment into Second Life."[78] Incredibly, that "deployment" helped London police crack down on a crime ring that had begun to sell stolen credit card information in virtual worlds.[79] Known as Operation Galician, the scheme allowed spies to rely on an informer who volunteered information he learned through his own digital avatar about the crime ring's activities.[80]

Alternatively, Australia has implemented a federal "co-regulatory scheme" that "enlists the cooperation of the government, the Internet industry, and the public to control Internet content."[81] That scheme operates on a complaint system, where a government body investigates complaints it receives and directs an ISP to remove any material deemed illicit.[82] That system is noteworthy because (a) if illicit content is hosted outside of Australia, the content is "referred

---

71 *Id.*
72 *Id.*
73 *Id.*
74 Danby, *supra* note 64, at 86.
75 *Id.*
76 *Id.* at 87.
77 *Id.*
78 Mazzetti & Elliott, *supra* note 10.
79 *Id.*
80 *Id.*
81 Vitale, *supra* note 37, at 110.
82 *Id.* at 110-11.

to vendors who manage filtering software and the content is added to a list of blocked materials"; and (b) the system turns content deemed illegal over to the host country.[83]

Furthermore, surveillance in Australia has also increased recently, taking a form more closely resembling the surveillance in the United States. For example, in just the first six months of 2012, the Australian government and its agencies made 523 requests to Google for access to its users' data.[84] Those numbers represent a steady rise in the number of requests since 2009, when Google first began to publish the requests it received.[85] More strikingly, Australian police are also obtaining citizens' "phone and internet records without warrants nearly 1000 times a week."[86] Those types of surveillance activities, which, for example, include information about Facebook use, resemble the U.S. National Security Agency's PRISM program.[87]

Many Australians question whether the NSA, through the PRISM program, relays information on Australian citizens in the United States to Australia.[88] Faced with such questions, Australian officials continue to caution that the government seeks to "balance the need of law enforcement agencies and their ability to investigate serious crime with the need to protect the privacy of personal communications."[89] Privacy advocates, however, are not optimistic that the government is restricting its own access to that information. They argue that it is reasonable to deduce that Australian agencies, as part of the "Five Eyes" agreement (which also includes the United States, the United Kingdom, Canada, and New Zealand), are sharing a wide range of information.[90]

However, because the Internet is not restricted by borders, domestic laws often do very little to curb Internet use among multiple countries, especially without "international assistance and consensus."[91] Since no country can force another to combat illegal activity, one of the most effective methods for fighting online crime is the establishment of international standards.[92]

Transnational organizations have also taken steps to address Internet crime. The European Union, for example, has taken an approach parallel to that of the United States. In 1995, the Council of the European Union adopted

---

83 *Id.*

84 *Australian Governments Increase Internet Surveillance*, AUSTRALIAN (Nov. 14, 2012), http://www.theaustralian.com.au/national-affairs/australian-governments-increase-internet-surveillance/story-fn59niix-1226516541141.

85 *Id.*

86 David Wroe, *Revealed: Internet Surveillance Rates*, SYDNEY MORNING HERALD (June 11, 2013), http://www.smh.com.au/it-pro/government-it/revealed-internet-surveillance-rates-20130610-2o07f.html.

87 *Id.*

88 *Id.*

89 *Id.*

90 *Id.*

91 Vitale, *supra* note 37, at 112.

92 *Id.*

requirements for telecommunications interception similar to those developed by the FBI.[93] It also urged both member states and non-member states to "implement the requirements with respect to systems and service providers in their own countries."[94]

Other transnational organizations, however, aim to foster cooperation between business and governments, and also between governments themselves. In the 1990s, the United Nations, by recommendation of the Eighth United Nations Congress on the Prevention of Crime and the Treatment of Offenders, "called upon Member States to intensify efforts to combat computer crimes."[95] In 2001, the General Assembly passed Resolutions 55/63 and 56/121, aimed at "[c]ombating the criminal misuse of information technologies."[96] Those resolutions "advocated the creation of a global framework to counter cybercrimes,"[97] and subsequent resolutions "encouraged Member States to create a global culture of cybersecurity and to take action to protect critical infrastructure."[98]

Similarly, the Council of Europe also seeks to "harmonize laws against cybercrime."[99] Its Convention on Cybercrime, which entered into force in 2004, originally sought to address the jurisdictional problems posed by the Internet.[100] It was introduced as "an international network of consistent laws [that] will improve national law enforcement's ability to react across borders and . . . restore the effectiveness of current crime control strategy."[101] In order to achieve its goals, it requires parties to amend their national laws to provide for "expedited preservation of stored data," "expedited preservation and disclosure of traffic data," "the ability to order a person to provide computer data under his or her control and to order a service provider to provide subscriber information under its control," "search and seizure of stored computer data," and "real-time collection of traffic data and interception of content data."[102] The Convention's execution, however, has been difficult, largely because its effectiveness relies on universal implementation, which has proven to be a difficult task.[103]

---

[93] James X. Dempsey, *Communications Privacy in the Digital Age: Revitalizing the Federal Wiretap Laws to Enhance Privacy*, 8 ALB. L.J. SCI. & TECH. 65, 117 (1997).

[94] *Id.*

[95] NIR KSHETRI, THE GLOBAL CYBERCRIME INDUSTRY: ECONOMIC, INSTITUTIONAL AND STRATEGIC PERSPECTIVES 18 (2010); G.A. Res. 45/121.

[96] KSHETRI, *supra* note 95, at 18.

[97] *Id.*

[98] *Id.*; G.A. Res. 57/239; G.A. Res. 58/199.

[99] KSHETRI, *supra* note 95, at 19.

[100] Amalie M. Weber, *The Council of Europe's Convention on Cybercrime*, 18 BERKELEY TECH. L.J. 425 (2003).

[101] Susan W. Brenner, *Cybercrime: Re-thinking Crime Control Strategies, in* CRIME ONLINE 12, 14 (Yvonne Jewkes ed., 2007).

[102] Jacqueline Klosek, *Convention on Cybercrime Raises Concerns about Data Privacy*, 6 No. 11 CYBERSPACE LAW. 2 (2002).

[103] Brenner, *supra* note 101, at 14.

Astutely, in its preamble, the Cybercrime Convention references international instruments that protect personal data.[104] These include "the 1966 United Nations Convention on Civil and Political Rights, the 1981 Council of Europe Convention for the Protection of Individuals with Regard to Automatic Processing of Personal Data, . . . and Recommendation No. (87) 15 regulating the use of personal data in the police sector."[105] Unfortunately, however, the Convention does not go beyond the lip service it pays to those institutions, and it fails to include the obligations the instruments impose.[106]

The Council of Europe has taken other measures to fight online crime as well. In 2008, for example, it established "voluntary guidelines to strengthen cooperation between police and Internet service companies."[107] The Council also aims to ensure that law enforcement in individual countries "follow[s] standard evidence-gathering techniques and promote[s] the use of the latest technology for tracking and catching cyber-criminals."[108]

On the other hand, the Council of Europe requires that its member countries provide "certain protections to personal data," as is required by some of its instruments, including the Data Protection Convention, and Recommendation No. (87) 15.[109] Interestingly, however, its signatories include Canada, Japan, South Africa, and the United States—countries that almost certainly afford less protection to personal data than the Cybercrime Convention requires.[110] This is because the Convention does not require countries outside the Council of Europe to meet those standards.[111] However, as a result of mutual assistance obligations contained in the Cybercrime Convention, citizens of countries within the Council of Europe, which are highly protective of personal data, may have their information transferred to countries outside the Council of Europe, which do not protect privacy as carefully.[112] Those risks raised such concerns for many members of the Council of Europe that the Data Protection Working Group established by European Community Directive 95/46/EC issued a special opinion recommending that the Convention contain provisions ensuring that people within the Council of Europe are not subject to less stringent privacy regulations.[113] That opinion, however, failed to persuade the Council, so the Cybercrime Convention contains only a "recital referencing the need to be mindful of the protection of personal data" and some "vague language concerning confidentiality and

---

104 Klosek, *supra* note 102.
105 *Id.*
106 *Id.*
107 KSHETRI, *supra* note 95, at 19.
108 *Id.*
109 Klosek, *supra* note 102.
110 *Id.*
111 *Id.*
112 *Id.*
113 *Id.*

limitation of use obligations related to mutual assistance requests."[114] Therefore, the Convention provides very little privacy protection to an individual's personal data.[115]

Finally, in 2000, the United Nations adopted the Convention against Transnational Organized Crime (UNTOC). The UNTOC provides member states with a framework for cooperating with each other to both prevent and combat organized crime.[116] Parties to the UNTOC commit to criminalizing activities such as "participating in an organized crime group, money laundering, corruption and obstruction of justice."[117] The parties must also adopt "sweeping frameworks" to assist with extradition, "mutual legal assistance," and "law enforcement cooperation."[118]

C. Relevant Concerns

1. Privacy

Concerns over privacy present a new battlefield in the ongoing debate about the relationship between law enforcement and individual privacy. That debate manifests itself in nearly every avenue of technological innovation. Most recently, the announcement of Microsoft's new gaming console, the Xbox One, sparked a wave of backlash because plans required the device to always be on and connected to the Internet.[119] The console also features a motion sensor system, called "Kinect 2," which has the ability to identify an individual's face and body, works in the dark, and records audio even when the console is turned off.[120] These technological capabilities suggest that the console could be used to monitor the number of people in a room.[121] Such reports incited backlash from those who feared the device could be used by corporations or governments to spy on people in their own homes even when they were not using the console.[122] In response to the backlash, Microsoft has since discarded the requirement that the Kinect 2

---

[114] Klosek, *supra* note 102.

[115] *Id.*

[116] *Organized Crime*, UNITED NATIONS OFFICE ON DRUGS AND CRIME, http://www.unodc.org/unodc/en/organized-crime/index.html (last visited Jan. 13, 2014).

[117] *Id.*

[118] UNITED NATIONS CONVENTION AGAINST TRANSNATIONAL ORGANIZED CRIME AND THE PROTOCOLS THERETO, http://www.unodc.org/unodc/treaties/CTOC/ (last visited Jan. 13, 2014).

[119] Evan Shamoon, *Xbox One Features Create Privacy Concerns*, ROLLING STONE (June 13, 2013), http://www.rollingstone.com/culture/news/xbox-one-features-create-privacy-concerns-20130613.

[120] *Id.*

[121] *Id.*

[122] *Id.*

system be turned on in order for the console itself to function.[123] Fear of similar surveillance activity has grown among the public in recent times, especially with the disclosure of the NSA's warrantless wiretapping as well as its policy of collecting metadata for phone calls through its PRISM program.[124]

Even more recently, the private sector has given new credence to these concerns. Eight leading tech companies, including Apple, Google, and Microsoft, released a nationwide joint statement in December 2013, pledging to strengthen encryption methods and resist heightened government surveillance efforts.[125] Such actions are partly a response to the concerns of customers, who are more distrusting of technology companies today, especially when the information such companies collect and use is the same information governments often seek to collect.[126]

In conjunction with these classical privacy concerns, increased surveillance of the Internet—and especially of VoIP services—raises new problems because of the way information travels across the Internet. While "phone networks by nature are closed and centralized, where all conversations between two parties traveled along a set path," information online "is distributed in data packets, which travel not on a set path, but by whatever route is available."[127] As a result, information is "broken up en route to the recipient's computer."[128] This structure makes it unclear whether the information contained in the transmission is "call-identifying information" or actual content.[129] Content information usually retains a higher level of protection than call-identifying information (or "signaling information" in relation to the Internet).[130] But, because VoIP services often package the two together, a legal search for one might improperly reveal the other and violate individual privacy.[131]

Additionally, expanding surveillance capabilities would likely involve the creation of "access points" on switches and routers, which in turn would make

---

[123] Keith Stuart, *Xbox One now Functions without Kinect Switched on – Confirmed*, GUARDIAN (Aug. 13, 2013), http://www.theguardian.com/technology/gamesblog/2013/aug/13/xbox-one-kinect-no-longer-switched-on.

[124] Timothy B. Lee, *Here's Everything We Know about PRISM to Date*, WASH. POST (June 12, 2013), http://www.washingtonpost.com/blogs/wonkblog/wp/2013/06/12/heres-everything-we-know-about-prism-to-date/.

[125] Edward Wyatt & Claire Cain Miller, *Tech Giants Issue Call for Limits on Government Surveillance of Users*, N.Y. TIMES (Dec. 9, 2013), http://www.nytimes.com/2013/12/09/technology/tech-giants-issue-call-for-limits-on-government-surveillance-of-users.html.

[126] *Id.*

[127] Gene D. Park, *Internet Wiretaps: Applying the Communications Assistance for Law Enforcement Act to Broadband Services*, 2 I/S: J.L. & POL'Y FOR INFO. SOC'Y 599, 613 (2006).

[128] *Id.* at 614.

[129] *Id.* at 615.

[130] *Id.*

[131] *Id.*

information more open to exploitation from both the government and third parties.[132] Requiring the establishment of access points would make "affected protocol designs considerably more complex," which "almost inevitably jeopardizes the security of communications even when it is not being tapped by any legal means."[133] As a result, private citizens may be able to illegally monitor one another with little guarantee that the government would prevent such behavior.[134] Third parties might also exploit those vulnerabilities to gain access to governmental communications.

These privacy concerns are compounded by the fact that people tend to "reveal more of [them]selves" online than through other modes of communication.[135] Because Internet users can often hide behind avatars and usernames, and because users do not know and will likely never meet the parties with whom they communicate, online activity appears (and often is) more anonymous. Consequently, some might perceive a greater expectation of privacy online. The idea that highly private or especially embarrassing information could be subject to inadequate security or incidental disclosure is particularly troublesome.

2. Innovation

A second issue arising from the prospect of increased Internet surveillance is the fear that surveillance programs may stifle domestic innovation. Such an effect might restrain domestic growth of an industry that continues to expand worldwide. In 2007, well over 200 million people played online games, and those users accounted for 28% of all people online.[136] Sales in online games "increase by a compound annual rate of 19.1%," and sales and revenue in 2008 brought in approximately 56 billion and 14 billion dollars a year, respectively.[137] The nearly 20% growth in sales dwarfs the growth rates for the film (7.5%), television (7.1%), and music (2%) industries during the same period.[138] The market for video games is nearly three times the size of the film industry.[139]

---

[132] Park, *supra* note 127, at 618.

[133] *Id.* at 618-19; NETWORK WORKING GRP., IETF POLICY ON WIRETAPPING (2000), *available at* http://tools.ietf.org/rfc/rfc2804.txt (noting that, in more complex systems, "the risk of unintended security flaws . . . is larger").

[134] Constance L. Martin, *Exalted Technology: Should CALEA Be Expanded to Authorize Internet Wiretapping?*, 32 RUTGERS COMPUTER & TECH. L.J. 140, 162 (2005).

[135] Susan Freiwald, *Online Surveillance: Remembering the Lessons of the Wiretap Act*, 56 ALA. L. REV. 9, 77 (2004).

[136] Duncan Riley, *217 Million People Play Online Games*, TECHCRUNCH (July 10, 2007), http://techcrunch.com/2007/07/10/217-million-people-play-online-games/.

[137] *Infiltrating a Virtual Gaming World*, *supra* note 33, at 6.

[138] *Id.*

[139] *Id.*

The primary concern with innovation is that a country that adopts restrictive regulations "could potentially drive technological innovations overseas."[140] Such an exodus would have significant economic implications because it would result in the loss of profitable technology and numerous technology jobs.[141] For example, if gaming companies were forced to comply with surveillance programs, they would have to spend significant resources developing compliance techniques rather than developing new products.[142] Instead of developing an idea and moving it to the market, innovators would need to consult with lawyers and intelligence officials, which would likely result in significant interference with the innovation process.[143] Similarly, without exposure to new technology as it is being developed, workforces in affected countries would likely fall behind others.[144] Also, without a global consensus on this issue, individual countries would have to implement their own policies one at a time, which may push customers—law-abiding and otherwise—away from using technology that they know has surveillance components and towards another country's software that they know is surveillance-free.

These are not new fears arising out of the current anti-surveillance political climate; they existed among encryption makers in the 1990s as well.[145] At that time, both the FBI and NSA argued that, unless they were given the ability to spy on "encrypted e-mails, IMs and phone calls," they would be unable to protect national security.[146] Only after a lengthy series of studies was the security community able to dissuade such spying.[147] Today, there is a similar fear among many that as long as the domestic government subjects innovators to regulation requirements, foreign providers "will enjoy an advantage."[148]

According to Susan Landau, a privacy and cryptography expert and a privacy analyst at Google, "[i]nnovation happens too fast on the internet to require companies that provide chat and voice-calling capabilities, which these days includes online games, social networking sites and a myriad of online chat and photo-sharing services, to comply with detailed wiretapping specifications that cost hundreds of dollars just to read."[149] To require, as the FBI suggests, Internet applications with communications systems to be "'vetted first will put American

---

[140] Martin, *supra* note 134, at 176.

[141] *Id.* at 177.

[142] *Id.*

[143] Christa M. Hibbard, *Wiretapping the Internet: The Expansion of the Communications Assistance to Law Enforcement Act to Extend Government Surveillance*, 64 FED. COMMC'NS. L.J. 371, 391 (2012).

[144] Martin, *supra* note 134, at 177.

[145] Hibbard, *supra* note 143, at 391.

[146] Ryan Singel, *FBI Drive for Encryption Backdoors Is Déjà Vu for Security Experts*, WIRED (Sept. 27, 2010), http://www.wired.com/2010/09/fbi-backdoors-2/.

[147] *Id.*

[148] Park, *supra* note 127, at n.22.

[149] Ryan Singel, *FBI Pushes for Surveillance Backdoors in Web 2.0 Tools*, WIRED (Feb. 17, 2011), http://www.wired.com/2011/02/fbi-backdoors/.

innovation at a global disadvantage.'"[150] Similarly, for any country to remain competitive, it must "preserve the ease and speed with which innovative new communications technologies can be developed."[151]

Additionally, Internet regulation raises concerns about its possible effect on the structure of the Internet itself. The Internet became a "fount of economic growth" largely because it enjoys a decentralized design: it exists separate from the control of any owner or centralized authority.[152] That design, however, contrasts with the "hub-and-spoke" design of traditional phone communication.[153] Requiring communications providers to be able to unscramble or intercept transmitted communications might reverse that design and negatively affect the "structure of the Internet in general."[154] Proponents of CALEA expansion consistently argue that "addressing the going dark problem does not require the Internet to be re-designed or re-architected for the benefit of the government."[155] On the other hand, ISPs claim that "asking institutions to provide a permanent back-door into the servers through which the government can access private information" would precisely require that type of restructuring.[156]

3. Free Speech

A third issue arising from Internet surveillance involves the potential it has to deter citizens from exercising free speech.[157] The fact that wiretap capabilities within Internet communications could be open to abuse creates inherent fears about exercising speech.[158] This chilling effect is detrimental not only to "the individual who is deterred from exercising his or her rights," but also to society in general, because "the uninhibited exchange of information, the active search for truth, and the open criticism of government are positive virtues."[159]

The immeasurable benefits of these positive virtues are as visible now as ever, especially given the role that social media played during the Arab Spring. In Tunisia, for example, two anonymous activists known only as "Foetus" and "Waterman" formed Takriz, a group that organized protests and disseminated

---

150 *Id.*

151 *Id.*

152 Hibbard, *supra* note 143, at 383.

153 *Id.*

154 *Id.*

155 Dell Cameron, *"Going Dark": What's So Wrong with the Government's Plan to Tap Our Internet?*, VICE (Apr. 3, 2013), http://motherboard.vice.com/blog/fbi-data-wiretap-trevor-timm-interview.

156 *Id.*

157 Gayle Horn, *Online Searches and Offline Challenges: The Chilling Effect, Anonymity and the New FBI Guidelines*, 60 N.Y.U. ANN. SURV. AM. L. 735, 743 (2005).

158 Hibbard, *supra* note 143, at 389.

159 Horn, *supra* note 157, at 749-50.

information using Facebook, Twitter, Skype, and Mumble.[160] Foetus called Facebook "the GPS for [the] revolution."[161] Protestors in Egypt followed suit, prompting the government to cut off Facebook and Twitter access and to eventually shut down nearly 90% of the country's Internet access.[162]

Even domestically, the chilling effect that many people fear may result from Internet regulation is not just a theoretical concern. Governmental surveillance is already proving to have a measurable impact on free speech rights. Recently, the Electronic Frontier Foundation submitted testimony from a diverse set of twenty-two activist groups, including Human Rights Watch, gun-rights activists, drug policy advocates, and Patient Privacy Rights,[163] alleging that the NSA's surveillance program is infringing on members' freedoms of speech and association.[164] In their testimony, the organizations claimed that, because their constituents no longer believe their communications are confidential, they have stopped using the services the organizations offer.[165] In addition, the organizations argued that as a result of the NSA's surveillance program, they have lost a significant part of their operational effectiveness.[166]

Also chief among free speech concerns is the idea that Internet surveillance might infringe on users' desires to remain anonymous. Such a desire not only involves being linked to speech, but also involves an individual's right to "have control over how he or she chooses to reveal him or herself, and control over the circumstances in which his or her speech is given."[167] Of course, some argue that online anonymity obstructs the prosecution of crime and harassment, allows for "people to avoid taking responsibility for their communications," and encourages offensive, defamatory, or harassing speech.[168] The "disadvantages caused by its abuse," however, "do not outweigh its significant benefits."[169]

One counter-argument some may make is that the "speech" that takes place in online games does not have the societal value of speech that occurs in

---

[160] Rebecca Rosen, *So, Was Facebook Responsible for the Arab Spring After All?*, ATLANTIC (Sep. 3, 2011), http://www.theatlantic.com/technology/archive/2011/09/so-was-facebook-responsible-for-the-arab-spring-after-all/244314/.

[161] *Id.*

[162] Christopher Williams, *How Egypt Shut Down the Internet*, TELEGRAPH (Jan. 28, 2011), http://www.telegraph.co.uk/news/worldnews/africaandindianocean/egypt/8288163/How-Egypt-shut-down-the-internet.html.

[163] Patient Privacy Rights is a nonprofit organization that seeks to increase Americans' control over their health records. *See* PATIENT PRIVACY RIGHTS, http://patientprivacyrights.org (last visited July 22, 2014).

[164] *EFF Files 22 Firsthand Accounts of How NSA Surveillance Chilled the Right to Association*, ELECTRONIC FRONTIER FOUND. (Nov. 6, 2013), https://www.eff.org/press/releases/eff-files-22-firsthand-accounts-how-nsa-surveillance-chilled-right-association.

[165] *Id.*

[166] *Id.*

[167] Horn, *supra* note 157, at 765.

[168] Hibbard, *supra* note 143, at 390.

[169] *Id.* at 390.

other public forums. Such an argument, however, discounts the immense influence that games have on society today, especially among younger generations. Some argue that their influence today among youth is "akin to that of the cultural influence of music, political movements and even religion on youth culture of the past."[170]

Additionally, it is clear that the potential chilling effect that online surveillance might have for the future is massive. With the ever-adapting nature of social media and online communities, and with the increasingly complex societies that arise within online games, it is worth protecting online speech now so that its constructive use persists in the future. Just a few years ago, the importance of protecting speech in areas like social media might have seemed absurd, but social media now plays an undeniable role in the dissemination of political, artistic, commercial, and educational speech. Today, over half of those who use Twitter get news from it, and thirty percent of adults say they get news from Facebook.[171] Additionally, singular "grassroots" political organizations like the Tea Party and Occupy Wall Street have roughly 124,000 and 185,000 "followers" on Twitter, respectively.[172]

Furthermore, constitutional precedent suggests that information exposed to the public deserves Fourth Amendment protection.[173] *United States v. Jones* reaffirmed that a person has a reasonable expectation of privacy regarding the information that a GPS would reveal about his whereabouts on public roadways.[174] In concurring with that decision, Justice Sotomayor expanded on the majority's analysis, noting that, in "the digital age, . . . people reveal a great deal of information about themselves to third parties in the course of carrying out mundane tasks," including "the phone numbers that they dial or text to their cellular providers; the URLs that they visit and the e-mail addresses with which they correspond to their Internet service providers; and the books, groceries, and medications they purchase to online retailers."[175] Regardless of the trade-off between privacy and convenience, and the perhaps "inevitable" diminution of privacy inherent in those transactions, she explains that it is doubtful "that people would accept without complaint the warrantless disclosure to the Government of a list of every Web site they had visited in the last week, or month, or year" merely

---

[170] R. Jayakanthan, *Application of Computer Games in the Field of Education*, 20 ELECTRONIC LIBRARY, no. 2, 2002, at 98.

[171] Jesse Holcomb et al., *News Use Across Social Media Platforms*, JOURNALISM PROJECT (Nov. 14, 2013), http://www.journalism.org/2013/11/14/news-use-across-social-media-platforms/.

[172] *Tea Party Patriots*, TWITTER, https://twitter.com/TPPatriots (last visited Jan. 14, 2014); *Occupy Wall Street*, TWITTER, https://twitter.com/OccupyWallStNYC (last visited Dec. 10, 2014).

[173] *See* United States v. Jones, 132 S. Ct. 945 (2012) (Sotomayor, J., concurring).

[174] *Id.* at 950 (majority opinion).

[175] *Id.* at 957 (Sotomayor, J., concurring).

because they had disclosed the information to "some member of the public for a limited purpose."[176]

Recently, the District Court for the District of Columbia extended this line of reasoning in *Klayman v. Obama*. The court delighted security activists everywhere when it refused to apply the landmark decision of *Smith v. Maryland*[177] to justify the NSA's telephony metadata program.[178] Finding that the program constituted what might be considered an unreasonable search, the court reasoned that "the evolutions in the Government's surveillance capabilities, citizens' phone habits, and the relationship between the NSA and telecom companies [are] so thoroughly unlike those considered by the Supreme Court thirty-four years ago that a precedent like *Smith* simply does not apply."[179] Many other decisions, however, support the position opposite those of both *Jones* and *Klayman*.[180]

4. Cost and Effectiveness

Finally, the prospect of conducting surveillance of online communications raises concerns about such a program's effectiveness because the vastness of online communications makes effective surveillance a daunting task. Perhaps the best known example of the challenge of collecting large amounts of data is the NSA's Utah Data Center. In order to keep up with the incredible amounts of data the center collects, it requires "65 megawatts of electricity and its own power substation."[181] Because of the heat generated by all of that power, the NSA uses "multiple chilling plants and 1.5 million gallons of water a day for cooling."[182] Still, despite the backup measures the NSA has taken, the center, which cost a billion dollars to build and costs over a million dollars a month to

---

[176] *Id.*

[177] 442 U.S. 735 (1979).

[178] 957 F. Supp. 2d 1 (D.D.C. 2013).

[179] *Id.* at 31.

[180] *See, e.g.*, Am. Civil Liberties Union v. Clapper, 959 F. Supp. 2d 724 (S.D.N.Y. 2013) (subscribers had no legitimate expectation of privacy in telephony metadata created by third party providers); United States v. Wahchumwah, 710 F.3d 862 (9th Cir. 2013) (a person has no expectation of privacy regarding information he voluntarily exposes to an undercover government agent in his own home); United States v. Graham, 846 F. Supp. 2d 384 (D. Md. 2012) (subscribers do not have a legitimate expectation of privacy in historical cell site location records for their cellular telephones); United States v. Alabi, 943 F. Supp. 2d 1201 (D. N.M. 2013) (defendants did not have a reasonable expectation of privacy in information electronically stored in magnetic strips on credit and debit cards found in their possession).

[181] Howard Berkes, *NSA Says It Has 'Mitigated' Meltdowns at Utah Data Farm*, NPR (Oct. 8, 2013), http://www.npr.org/blogs/thetwo-way/2013/10/08/230520905/nsa-says-it-has-mitigated-meltdowns-at-utah-data-farm.

[182] *Id.*

operate, experienced ten "meltdowns" in thirteen months.[183] Though the NSA surveillance programs may involve the collection of a larger amount of data when compared to online surveillance programs, the former only collects data on a closed network with distinct start and end points. Therefore, the type of communications that exist in online games might be even harder to compile.

But the problems with storing large amounts of data are not the only obstacles standing in the way of effective online surveillance. Even increased surveillance capabilities may not effectively give law enforcement agencies the ability to collect the information they need. This is because the Internet allows criminal organizations to communicate and expand beyond borders. Relevant communication, therefore, may often involve multiple jurisdictions that fall outside the scope of one agency.[184] Criminal organizations understand the problems that these jurisdictional issues pose, and they often function in jurisdictions that have few laws and little capacity to enforce them.[185] As a result, effective local enforcement may often prove impossible.[186]

Additionally, the "architecture of the Internet also lends itself to vulnerabilities and makes it more difficult to wiretap" on a manageable scale.[187] Expanding surveillance programs like CALEA to the Internet would consequently "require a different and more complicated protocol, which would create serious security problems."[188] Furthermore, because "[t]he Internet is easier to undermine than a telephone network due to its 'flexibility and dynamism,'" incorporating means for surveying its use would "build security vulnerabilities into the communication protocols."[189] Attempts to add similar features in the past have "resulted in new, easily exploited security flaws rather than better law enforcement access."[190]

Moreover, Internet surveillance would likely cost a significant amount of money, much of which would be foisted upon online companies themselves.[191] Consequently, not only would expanded surveillance lead to a "technology and security headache," but the "hassles of implementation" and "the investigative burden and costs will shift to providers."[192]

---

[183] Rory Carroll, *NSA Data Centre Opening Delayed after Series of Electrical Surges in Utah*, GUARDIAN (Oct. 8, 2013), http://www.theguardian.com/world/2013/oct/08/nsa-data-centre-utah-electrical-surge.

[184] *Going Dark*, *supra* note 19, at 5.

[185] Phil Williams, *Organized Crime and Cyber-Crime: Implications for Business*, CERT COORDINATION CENTER (2002) (on file with author).

[186] *Id.*

[187] Hibbard, *supra* note 143, at 384.

[188] *Id.* at 384.

[189] *Id.* at 385.

[190] *Id.*

[191] *Id.* at 390.

[192] Hibbard, *supra* note 143, at 390.

Despite those concerns, however, online surveillance might be less costly and more effective than traditional wiretapping.[193] Online surveillance allows for large quantities of data to be "gathered at minimal cost, either as it is produced or at some time later."[194] Additionally, though the development of computerized surveillance systems may be difficult, once created, they "may be duplicated at a fraction of the cost."[195] Further, online surveillance potentially makes identifying users easier because the content discovered often includes identifying information, like IP addresses.[196] Finally, electronic surveillance may prove efficient for law enforcement because it does not require "contemporaneous listening."[197] Unlike traditional wiretapping, where agents listen to conversations live and stop recording if the conversations do not contain criminal content, electronic surveillance seems to require only "after-the-fact filtering," which eliminates the need to have an agent monitor communications in real time.[198] Thus, because online surveillance "offers cheaper, richer, and more reliable information with less risk," its use might be more effective than other evidence-gathering techniques, especially "to the extent that law enforcement agents [can] focus their efforts on a particular person who spends time online."[199]

III. ANALYSIS

Taking the above considerations into account, governments must mull over a number of options and relevant questions regarding the effectiveness of transnational information-sharing and governing bodies as well as the relative usefulness of domestic surveillance law like the proposed expansion to CALEA. In addition, governments must consider whether individual agents would provide an effective—and less invasive—tool for information gathering and whether private entities like the companies who create and operate the games can function as an effective tool for deterring and reporting illegal activity.

A. The Usefulness of Uniform International Guidelines

Centralized bodies, such as the U.N. Office on Drugs and Crime (UNODC) and the International Chamber of Commerce Commercial Crime Services, have effectively combated international crime, and they may effectively centralize efforts to reduce organized crime online. The UNODC in particular is

193 Freiwald, *supra* note 135, at 43.
194 *Id.*
195 *Id.*
196 Martin, *supra* note 134, at 172
197 Freiwald, *supra* note 135, at 43.
198 *Id.*
199 *Id.* at 44.

in a prime position to combat criminal organizations online. A central monitoring body created within the UNODC might prove useful for a number of reasons. For one, its position within the United Nations would allow it to function as a "neutral forum" for representatives from countries affected by international organized crime, business leaders, and law enforcement agencies.[200] In those situations, the UNODC "could operate as an arbitrator in discussions between countries to determine appropriate Internet regulation" without running into jurisdictional problems.[201] Such a forum would also give countries direct access to foreign ISPs so that they could more easily coordinate law enforcement efforts. By "observing and regulating Internet activity, addressing concerns from nations, and making changes to monitoring schemes," a central monitoring body would more uniformly regulate Internet use.[202]

Even so, there is a risk that such a body would meet resistance among many members of the international community. Not only would a regulatory body raise the concerns mentioned in part II(C), especially regarding freedom of speech, but coordinating efforts within a body as large as the U.N. also poses a significant barrier to effective regulation because of the difficulty in generating consensus among so many members. Individual countries that refuse to comply with the requisite regulations might provide a haven for criminal organizations. In order to prevent such a situation, a centralized body would likely need to provide significant incentives for countries to comply.

Unfortunately, international agreements often prove ineffective because of their inability to create cohesive and effective cooperation that includes all members and takes into account the situational differences that various countries face. Because coordinating large institutions is difficult, it is likely that soft spots would emerge inside the agreements. As long as those spots exist, criminal organizations will be able to find a safe haven within them. As a result, law enforcement agencies will likely have more success with other strategies because of the difficulty inherent in establishing a coordinating body and the likelihood that it will be ineffective.

B. International Treaties and Intelligence-sharing

One of the most promising options in the fight against organized crime online are international treaties, which have the ability to coordinate international efforts so that governments can share information and more efficiently address international crime. Implementing such agreements, however, has raised significant concerns for law enforcement. The Convention on Cybercrime, for example, contains forty-eight articles, of which thirty-three require parties "to

---

200 Vitale, *supra* note 37, at 128.
201 *Id*.
202 *Id.*

adopt legislation or take other implementing measures."[203] As a result, complying with the treaty is a burdensome task for countries that do not already have cybercrime laws in place.[204] Even more complicating is the fact that the Convention, like many international agreements, addresses the online crime problem from a narrow viewpoint: that of the United States and Europe.[205] As a result, countries with different local laws and cultures may have difficulty adjusting to the substantive and procedural law that the treaty contains.[206] And even if each country successfully implements a treaty's provisions, the ever-evolving nature of technology may render those provisions obsolete in a matter of years.[207] So far, many parties to the Convention have failed to enact the requisite criminal statutes and still lack the resources necessary to conduct adequate investigations.[208] Furthermore, the mutual assistance provisions in the treaty have failed to foster adequate cooperation between the parties.[209]

Additionally, the Convention raises many of the privacy concerns inherent in information-gathering efforts. Not only does it allow for the collection of personal information and the monitoring of information systems, but it also allows for the exchange of large amounts of sensitive data between countries, "some of which have lesser standards of privacy and data protection standards than others."[210] Although the Convention mandates that its provisions be subject to the safeguards "'provided under the domestic law of each Party concerned,' it does not require that any such conditions of safeguards actually be in place."[211]

Similarly, these privacy concerns arise out of many information-sharing agencies because they often suffer from problems that result from the structure of the agencies themselves. Because of the way these agencies are organized, they often become abusive.[212] Such agencies are often "[c]haracterized by secrecy, flexibility, and informality," and they often function outside the structures of law.[213] As a result, information-sharing networks, which "essentially regulate themselves," suffer from a lack of responsibility that, at worst, may threaten the ideals of liberal democracy that those structures protect.[214]

While, on their face, information-sharing networks functioning within their own legal constraints may appear innocuous, networks that can effectively address the wide-ranging problems posed by organized crime on the Internet will

---

203 Brenner, *supra* note 101, at 18.
204 *Id.*
205 *Id.*
206 *Id.*
207 *Id.*
208 Weber, *supra* note 100, at 427.
209 *Id.*
210 Klosek, *supra* note 102.
211 *Id*.
212 Elizabeth Sepper, *Democracy, Human Rights, and Intelligence Sharing*, 46 TEX. INTL. L.J. 151 (2010).
213 *Id.*
214 *Id.* at 153.

need to draw from a wide array of sources. Currently, "virtually no other mechanism provides oversight or accountability for an intelligence agency's transnational activities," and that problem will only grow worse as scale increases.[215] Additionally, information-sharing networks experience little oversight or regulation because elected officials often fail to understand the intricacies of intelligence cooperation.[216] As a result, "agencies can circumvent domestic and international legal restraints and collude with one another to the detriment of their respective states."[217]

Furthermore, intelligence agencies are incredibly complex, often most closely resembling spider webs with "a multiplicity of connections expanding in every direction" rather than one-on-one or hub-and-spoke designs.[218] As a consequence, single agencies "may have hundreds of ties and relationships to counterpart agencies worldwide," as is the case with the Canadian Security Intelligence Service (CSIS), which, despite its small institutional size, "has more than 250 information sharing arrangements with foreign security and intelligence organizations."[219] In the case of the U.S. Central Intelligence Agency (CIA), those connections reach more than 400 agencies.[220] Because of their size, networks like those reach far beyond their individual agency's resources, giving officials access to information they might not otherwise have or be legally entitled to obtain.[221] Furthermore, intelligence networks "operate with the highest levels of secrecy."[222] Not only are the "very structures through which agencies share information" secret, but the essential elements, including "the participants, methods of operation, and agreements themselves," are secret as well.[223] That scope and secrecy makes effective oversight even less likely.

This lack of oversight is most dangerous because of the relationships through which intelligence agencies share information. The majority of the intelligence that these agencies share does not transfer through formal, multilateral agreements.[224] Instead, agencies share information "through informal, typically bilateral network arrangements."[225] Often times, those arrangements establish a "loose and adaptable framework in which to share information, ideas, and resources."[226] These informal agreements allow contact "even when interaction

---

215 *Id.*
216 *Id.*
217 Sepper, *supra* note 212, at 153.
218 *Id.* at 155
219 *Id.*
220 *Id.*
221 *Id.*
222 Sepper, *supra* note 212, at 156.
223 *Id.* at 156-57.
224 *Id.* at 158.
225 *Id.*
226 *Id.*

with a certain intelligence agency (or state) is officially disfavored" because they frequently operate "below the level of official control."[227]

Because of these characteristics, "even though intelligence agencies regularly cooperate with one another, their network arrangements are nearly invisible to national publics, legislators, and international bodies."[228] As a result, intelligence agencies are insulated from criticism, seldom reprimanded for failures to effectively share intelligence, and rarely at risk of major repercussions for bad intelligence.[229] Moreover, intelligence agencies often lack democratic accountability because they are immune from effective oversight.[230]

As a result of the institutional problems inherent in information-sharing organizations, they continue to cooperate "without public knowledge, legislative consent, or even executive approval"—a problem that is only exacerbated by the "perpetual secrecy of information shared through networks."[231] Consequently, the problems raised by increased information-sharing would likely outweigh its benefits.

C. Expansion of Domestic Surveillance Capabilities

Law enforcement agencies contend that a system providing law enforcement with the ability to track data relating to online games—like CALEA—has obvious benefits. According to NSA reports, even though games appear to be "unregulated digital bazaars," the companies running them often enforce a rigid set of monitoring capabilities.[232] Those companies both "reserve the right to police the communications of players and store the chat dialogues in servers" and monitor "transactions conducted with the virtual money common in the games" in order to prevent "illicit financial dealings."[233] Those logs can be searched later to reveal valuable information.[234]

In fact, NSA sources report that, by monitoring World of Warcraft (WoW), it has been able to "uncover potential [SIGINT][235] value by identifying accounts, characters and guilds related to Islamic extremist groups, nuclear proliferation and arms dealing."[236] This practice, at the very least, appears to

---

[227] Sepper, *supra* note 212, at 158-59.

[228] *Id.* at 168.

[229] *Id.*

[230] *Id.*

[231] *Id.*

[232] Mazzetti & Elliot, *supra* note 10.

[233] *Id*.

[234] *Id*.

[235] SIGINT is short for "Signals Intelligence," which refers to "collecting foreign intelligence from communications and information systems and providing it to" government officials. *SIGINT Frequently Asked Questions,* NAT'L SEC. AGENCY (Jan. 15, 2009), http://www.nsa.gov/sigint/faqs.shtml.

[236] Mazzetti & Elliot, *supra* note 10.

allow intelligence agencies to identify targets of interest who are playing games, even if the agencies have not identified illicit activity within the games.[237] Similarly, British intelligence has "successfully been able to get the discussions between different game players on Xbox Live."[238]

Systems like these, however, have implications beyond identifying individual criminals who are operating online. Some in the intelligence community have discussed the possibility of identifying dangerous individuals based on online behavior. In 2009, academics and defense contractors presented proposals for a government study about "how players' behavior in a game like World of Warcraft might be linked to their real-world identities."[239] Such a tool might be valuable if intelligence agencies can confirm that criminals are "using virtual spaces to communicate or coordinate."[240] Whether such research would be useful is unclear. One group, for example, found that "younger players and male players [prefer] competitive, hack-and-slash activities, and older and female players [prefer] noncombat activities."[241] A second found that "players under age 18 often used all capital letters both in chat messages and in their avatar names."[242] It is unlikely that either of those revelations will help law enforcement catch any criminal masterminds.

Still, analysis of metadata has led to some promising developments for intelligence agencies. The NSA reports that WoW's "gaming format can provide a virtual organizational platform for potential SIGINT targets," and can "assist the SIGINT community in tracking that target."[243] Additionally, the infrastructure of WoW itself provides a wealth of information regarding a person's network that can be obtained "through the data passed during WoW messages, such as country and time zone information, local IP addresses and realm server addresses."[244]

Collecting that type of in-game intelligence through the monitoring of "in-game activities and related game-devoted areas of the Internet" provides intelligence agencies with significant opportunities.[245] For example, they might be able to identify financial operations by "monitoring the flow of money in virtual economies and determining who is involved in the buying and selling of virtual goods and fundraising."[246] Thus, if criminals sell virtual goods for real money or if they transfer account details between each other in order to transfer

---

237 *Id*.
238 *Id*.
239 *Id*.
240 *Id*.
241 Mazzetti & Elliot, *supra* note 10.
242 *Id*.
243 *GVE Paper*, *supra* note 15.
244 *Id*.
245 *Id*.
246 *Id*.

goods among themselves, law enforcement would be able to track the distribution of those goods and the transactions.[247]

However, law enforcement agencies still argue that they need expanded access to in-game information in order to make the interception of such information easier. At present, agencies have difficulty distinguishing gaming data from other Internet traffic.[248] And the time it takes them to uncover relevant data often keeps law enforcement from effectively prosecuting their targets. As a consequence, they have made a number of recommendations. Chief among those are the expansion of intelligence-gathering loopholes that will open communications for monitoring.

Privacy advocates, however, stridently refuse to permit such changes. For one, they refute the idea that those changes would significantly help law enforcement agencies. Despite the potential value that increased Internet surveillance might have, surveillance of games has yet to produce consistent success.[249] In fact, former intelligence officials, as well as current and former gaming company employees, have reported little evidence indicating that anyone has been able to identify criminal groups communicating within games.[250]

Instead, privacy advocates argue that back-door access points that would make it easier to survey games would make the public as a whole less safe. During the "crypto wars" of the 1990s,[251] the security community managed to demonstrate that "national security was actually strengthened by wide use of encryption to secure computers and sensitive business and government communications."[252] They continue to draw support from a 1996 National Research Council report finding that "requiring back doors was not a sensible policy for the government."[253] Therefore, the proper action to take, they argue, would be to increase the protection for individuals and businesses.[254] Such is the case because "[b]uilding wiretapping into communications infrastructure creates serious risk that the communications system will be subverted either by trusted insiders or skilled outsiders," such as foreign governments, hackers, and identity thieves.[255]

While privacy advocates admit that the spread of encryption technologies would "add to the burden of those in government who are charged with carrying

---

247 *GVE Paper*, *supra* note 15.

248 Mazzetti & Elliot, *supra* note 10.

249 *Id*.

250 *Id*.

251 *See supra* text accompanying notes 145-147.

252 Singel, *FBI Drive for Encryption Backdoors Is Déjà Vu for Security Experts*, *supra* note 146.

253 *Id*.

254 *Id*.

255 Singel, *FBI Pushes for Surveillance Backdoors in Web 2.0 Tools*, *supra* note 149.

out certain law enforcement and intelligence activities," they argue that the benefits to society of widespread privacy measures outweigh the disadvantages.[256]

Finally, many question the reality of the "going dark" problem[257] about which the FBI complains. As Trevor Timm, Executive Director of the Freedom of the Press Foundation, explains, "we've never really seen any actual evidence that [the going dark problem] actually exists."[258] The FBI and the Department of Justice (DOJ) have to report the number of times "they run into encryption when they ask for surveillance," and in each of the last eleven years, that number has been zero.[259] Additionally, both organizations have "a multitude of ways" of gathering information, and reports indicate that "government surveillance on the Internet is actually on the rise."[260] In fact, according to the government's own record, "cases of encryption tripping up law enforcement are extremely rare."[261] For example, the government obtained court approval for 2,376 wiretaps in 2009, and it encountered encryption only once.[262] Despite the encryption, the government was still able to uncover the contents of the communication in question.[263] In other years, the government ran into "no problems whatsoever."[264]

Given the numerous privacy, security, and innovation concerns apparent in expanding domestic surveillance capabilities, such measures will likely prove unhelpful. As a result, governments will likely benefit from a "hands-off" approach, relying on game creators themselves to police their virtual worlds and using the capabilities that game creators already have to ensure that criminal organizations cannot use online games to thrive in other areas.

D. The Usefulness of Monitoring and Moderation by Game Creators

In light of the difficulties that outside agencies would face in attempting to monitor online games, the most effective crime prevention entities would likely be the game creators themselves. For example, companies that control the software and servers that run online games could monitor in-game communication for signs of illegal activity and report suspicious activity to relevant law enforcement officials. By cooperating with law enforcement, private companies

---

256 Singel, *FBI Drive for Encryption Backdoors Is Déjà Vu for Security Experts*, *supra* note 146.

257 *See supra* notes 19-23.

258 Cameron, *supra* note 155.

259 *Id.*

260 *Id.*

261 Singel, *FBI Drive for Encryption Backdoors Is Déjà Vu for Security Experts*, *supra* note 146.

262 *Id*.

263 *Id*.

264 *Id*.

like these can help identify criminal users and activities, counter crimes themselves, and generally make the online realm a safer place.[265]

Such a system would have a number of advantages over the alternatives. For one, the private companies that developed the games are the entities most familiar with their technology and with the games themselves. Thus, they would most easily be able to monitor and control the activity that takes place online, and they could best distinguish common types of activity from possible criminal activity.

Second, this system would avoid many of the security concerns raised by outside surveillance. Relying on gaming companies to identify and control relevant criminal information would permit law enforcement to use the information they gather to prosecute criminal organizations without subjecting the broad gaming population to the security weaknesses that result from other aids to law enforcement, such as "back-door" access points or lower levels of encryption.[266]

Third, this system would avoid placing the substantial burden of monitoring all relevant gaming communications on a small number of government organizations. Rather than rely on governments or law enforcement agencies—many of whom already suffer from a lack of resources—to sift through the vast collection of online gaming, this system would split that responsibility among many different groups who could then focus on their own users without gathering new resources, dedicating new departments, or worrying about jurisdictional concerns. Therefore, gaming companies could more efficiently monitor online communications.

Most importantly, companies who run online games already have the ability to, and currently do, moderate their users' communications. Gaming companies already reserve the right to "police" communications and "store" chat dialogues on their servers, which they can access at a later time.[267] Some companies also keep track of the virtual money their users spend.[268] Microsoft uses a similar system to enforce its code of conduct, which prohibits users from engaging in criminal activity and allows the company to suspend the accounts of those who commit violations.[269] In a similar vein, Facebook monitors its users' chats and occasionally relays suspicious information to police.[270]

---

[265] *Cyber Crime – A Growing Challenge for Governments*, KPMG ISSUES MONITOR, July 2011, at 15, *available at* https://www.kpmg.com/Global/en/IssuesAndInsights/ArticlesPublications/Documents/cyber-crime.pdf.

[266] *See supra* Part II.C.1.

[267] Mazzetti & Elliot, *supra* note 10.

[268] *Id.*

[269] Xbox Live Code of Conduct, MICROSOFT (last updated Jan. 2014), http://www.xbox.com/en-US/legal/codeofconduct.

[270] *Law Enforcement & Third-Party Matters*, FACEBOOK, https://www.facebook.com/help/473784375984502 (last visited Mar. 23, 2014); *see also* Joseph Menn, *Social Networks Scan for Sexual Predators, with Uneven Results*, REUTERS

Of course, such a system would not be without drawbacks as well. Relying on private companies to repost activity themselves raises the possibility that they could neglect to monitor their users or that they could underreport likely criminal activity. However, law enforcement agencies should take steps to establish a relationship with game creators to ensure that the creators take measures necessary to identify and report suspicious activity. For these reasons, such private companies would provide the most effective resource for combating criminal organizations that use online games.

IV. CONCLUSION

As the realm of online gaming continues to evolve, the opportunities provided by online games—for both criminal organizations and law enforcement—will change along with it. U.S. intelligence agencies predict that "[a]s virtual worlds become more popular, pervasive, and sophisticated," so will the efforts of criminal groups to exploit them.[271] The NSA goes so far as to suggest that, in the near future, it will be easier for terrorist groups to reach core target audiences through the use of the ever-increasing access to gaming platforms provided by "personal computers, Internet cafes, and mobile platforms" than to recruit face to face.[272] As a result, terrorist groups will "increasingly leverage online and computer based games to support their activities in the future."[273] Such opportunities, the NSA insists, will include "strategic propaganda and influence activities," "instrumental uses such as communication, fundraising and recruitment," and even highly complex practical uses, such as planning and practicing attacks in virtual environments.[274] Therefore, the NSA claims that the "increasing popularity of gaming which seems to be transcending age, gender, and cultural boundaries" is a cause for concern.[275] Even if those threats seem slightly overblown, it is clear that the potential abuse afforded by communication in online games presents, at the very least, a credible threat to public security interests. Consequently, "doing nothing" is simply not a viable option.

Given the unique nature of the online gaming environment, agencies that attempt to combat organized crime online will encounter a number of procedural and technological obstacles. In addition, each plausible option available to intelligence agencies implicates significant governmental and societal concerns. An effective crime-fighting strategy must take address those concerns.

(July 12, 2012), http://www.reuters.com/article/2012/07/12/us-usa-internet-predators-idUSBRE86B05G20120712.

[271] *Infiltrating a Virtual Gaming World*, *supra* note 33, at 12.

[272] *Id.*

[273] *Id.*

[274] *Id.* at 30.

[275] *Id.*

As with most information-gathering techniques, probing into the various communications related to online gaming means potentially invading the privacy of millions of users or subjecting users' communications to vulnerabilities that third parties could exploit. Consequently, any measures that law enforcement agencies take will need to consider for those drawbacks.

Furthermore, subjecting gaming technology to stricter surveillance standards risks retarding innovation within the countries that impose such higher standards, inflicting disproportionate burdens on compliant companies, and slowing any economic growth resulting from a burgeoning industry. As a result, regulatory measures must not overstrain game developers for fear of driving them out of a country's gaming industry.

Additionally, the vastness of gaming communication means that attempts to sort through data will give rise to significant cost-effectiveness obstacles. Law enforcement agencies must always be worried about losing relevant evidence in the deluge because of the difficult nature of sorting relevant gaming data from non-relevant data, monitoring its real-time development, and deciphering its beginnings and endpoints.

Finally, as online gaming continues to grow and evolve, its status as a forum for speech will grow with it. Therefore, crime-fighting measures should take care not to smother what may grow into a potentially valuable medium of expression. Because much of the Internet thrives on anonymity and free expression, governments should strive to avoid violating or fundamentally altering the principles upon which it was founded.

Given these concerns, the possible remedies available to law enforcement bodies—the establishment of uniform standards governed by intergovernmental bodies, the practice of information-sharing, increased domestic surveillance capabilities, and private monitoring—all raise important issues. For one, uniform international standards for combating cybercrime would likely fail to adequately address the issue. Because international organizations often fail to function effectively without universal compliance, the practical solutions those organizations provide would fall short of their goals. Additionally, broader governmental surveillance is not a reasonable option. Such programs raise threats to privacy, innovation, and free speech that may outweigh the benefits they provide. Finally, given the logistical concerns inherent in the structure of the Internet, the organization of online games, and the ineffectiveness of broad intergovernmental organizations, information sharing between governmental surveillance programs would likely fail to achieve desirable results.

Consequently, the task of regulating online communications should be left to game creators themselves. They are in the best position to effectively monitor the activities of their customers; they would be able to implement security measures across their own networks without having to take into consideration the sovereignty of their customers' countries; and, because they must answer directly to their customers for fear of losing business, they would constantly need to respond to their customers' concerns about privacy and expression.