THE DARK WEB AND EMPLOYER LIABILITY

DAVID D. SCHEIN*

LAWRENCE J. TRAUTMAN**

The World Wide Web ("WWW") is a dominant force in the lives of many. It provides access to a range of services and information from email access to shopping to social media to instant information on search engines like Google. For most persons using the WWW, this is all there is to the Internet and in fact, perhaps many could do with a great deal less contact through Facebook and other social media. However, there is more to the Internet than the WWW. Some sources suggest that the non-WWW part of the Internet may be even larger than the WWW part. "The Dark Web" is the term used most often for the remainder of the Internet. The Dark Web provides a source for many contraband or illegal items, including weapons, drugs, pedophilia, ransomware, stolen identities, and tools for terrorism. The reason for the growth of The Dark Web has been the possibility to use this avenue anonymously, unlike the WWW. The coin of this realm is the Bitcoin, the untraceable virtual currency. For employers, allowing employees access to The Dark Web using computers and laptops, or even mobile phones, provided by the employer is a growing source of liability. This article explores the growing legal risks for employers.

Keywords: AlphaBay, Bitcoin, Carpenter, Criminal Law, Darkode, Dark Web, Employer Liability, Fourth Amendment, Hansa, Internet, Jardines, Jones, Kahler, Katz, Kyllo, PlayPen, Ransomware, Riley v. California, Silk Road, Virtual Currencies

* BA, University of Pennsylvania; MBA, University of Virginia; JD, University of Houston Law Center; Ph.D., University of Virginia. Professor Schein is Associate Dean, Director of Graduate Programs, and Associate Professor, Cameron School of Business, University of St. Thomas, Houston, Texas. He may be contacted at ScheinD@stthom.edu.

** BA, The American University; MBA, The George Washington University; JD, Oklahoma City University School of Law. Professor Trautman is Associate Professor of Business Law and Ethics at Prairie View A&M University. He may be contacted at Lawrence.J.Trautman@gmail.com.

JEL Classifications:

OVERVIEW

The World Wide Web ("WWW") is a dominant force in the lives of many, providing access to a range of services and information. These include: email access, shopping, social media, and instant information on search engines like Google, to name just a few. For most persons using the WWW, this is all that there is to the Internet and in fact, many could perhaps do with a great deal less contact through Facebook and other social media. However, there is more to the Internet than the WWW. Some sources suggest that the non-WWW part of the Internet may be even larger than the WWW part. "The Dark Web" is the term used most often for the remainder of the Internet. The Dark Web provides a source for many contraband or illegal items, including: weapons, drugs, pedophilia, a launching pad for ransomware, tools for terrorism, and sales of stolen identification information. The reason for the growth of The Dark Web has been the ability to use this avenue anonymously, unlike the WWW. The coin of this realm presently is virtual currencies, the most prominent being the Bitcoin, the untraceable virtual currency. At the same time, some employees may be using The Dark Web to protect their identity while they gather material for sensitive articles or for whistleblowing. Further, law enforcement agencies around the world have engaged in sophisticated hacking campaigns to track down the persons using The Dark Web for illegal purposes. For employers, allowing employees access to The Dark Web while using computers and laptops, or even mobile phones, provided by the employer is a growing source of liability. In Part I, this article provides an introduction to the structure of The Dark Web and its operations. In Part II, we examine the many negative aspects of The Dark Web, including terrorist plots, gun dealing, drug dealing, pedophilia, ransomware, and sale of stolen identities. In turn, this article reviews the reported positive uses of this part of the Internet. In Part III, we examine recent court rulings related to the illegal activities referenced above that provide an idea of the types of risks for employers. Finally, Part IV presents recommendations for the future concerning employers and The Dark Web. This Article contributes to the existing literature by discussing the criminal activities taking place on The Dark Web and by explaining the possible cyber threats employers face.

I. THE INTERNET AND DARK WEB

The Internet began in 1989 as an association of academics who connected their computers to exchange knowledge.[1] While growth during that first decade was slow, many entrepreneurs began to understand and develop the business of the Internet, including email services that originally charged for the privilege to access the users' email accounts and to perform simple searches.[2] The growth over the last 20 years has been nothing less than a worldwide phenomenon. It is estimated that 90% of Americans have at least some level of Internet service.[3] Worldwide, a recent estimate indicates that over 51.2% of the global population has Internet access.[4] Daily use of the Internet through the portal known as the World Wide Web provides access to email, shopping, research, games, maps, and social media. In addition, "apps," short for applications, quickly connect users to an enormous number of vendors and services, including airlines, hotel chains, and of course, social media platforms.

A. Development of The Dark Web

Not surprisingly, the growth of the Internet and specifically, the growing popularity of the "Bitcoin," a virtual currency,[5] have led to the development of The Dark Web.[6] Bitcoin's role in the growth of The Dark Web is explained simply by the fact that when cash is transmitted electronically, it leaves a trail of who sent and who received. Furthermore, alternative cash vehicles like credit cards and checking accounts must be associated with businesses or individuals in some fashion, so, unlike Bitcoin, anonymously

1. *History of the Web*, WORLD WIDE WEB FOUNDATION, https://webfoundation.org/about/vision/history-of-the-web/ [https://perma.cc/GR33-UP62] (last visited June 7, 2019).

2. *Why Pay for Email*, RUNBOX SOLUTIONS AS, https://runbox.com/why-runbox/why-pay-for-email/ [https://perma.cc/LT4X-KJMB] (last visited June 7, 2019).

3. Monica Anderson et al., *10% of Americans Don't Use the internet. Who Are They?*, PEW RESEARCH CTR. (Apr. 22, 2019), http://www.pewresearch.org/fact-tank/2018/03/05/some-americans-dont-use-the-internet-who-are-they/ [https://perma.cc/WYG5-U27K].

4. Press Release, Int'l Telecomm. Union, ITU Releases 2018 Global and Regional ICT Estimates (Dec. 7, 2018).

5. *See* Sharon Yin, *Cryptocurrencies an Evolving Ecosystem is Changing the Way Society Transfers Value,* 81 TEX. B. J. 324 (2018).

6. Axel Bugge, *Dark Web Drug Market Growing Rapidly in Europe: Report*, REUTERS (Nov. 28, 2017), https://www.reuters.com/article/us-europe-drugs-darkweb/dark-web-drug-market-growing-rapidly-in-europe-report-idUSKBN1DS28A [https://perma.cc/U63E-59PP].

purchasing weapons,[7] pedophilia,[8] drugs,[9] or stolen identity information[10] is not easily accomplished because there is not an untraceable common means of exchange.

Around the world, law enforcement is using special investigative techniques to attempt to detect and apprehend the vendors of the illegal materials on The Dark Web—one such tool is the "Network Investigative Technique" ("NIT").[11] The NIT is a sophisticated form of hacking by law enforcement and intelligence agencies.[12] These agencies work through vulnerabilities in The Dark Web to identify those who do not wish to be found.[13] The use of the NIT and similar devices is discussed in Part III, below. The NIT has garnered criticism from academics and civil rights activists because while a general search warrant applies to the granting judge's geographical area, the NIT can cover a much wider geographic area, and can even extend outside the United States.[14]

B. Tor ("The Onion Router")

As The Dark Web is not accessed by customary web browsers, access to it requires a special approach. The main route is through The Onion Router, known simply as "Tor."[15] One of the ironies of Tor is that it was developed not by a group of hackers but by the United States Naval Research Lab in the 1990s, as a pipeline to

7. *See generally* United States v. Focia, 869 F.3d 1269, 1274-76 (11th Cir. 2017) (discussing The Dark Web market and the purchase of firearms).

8. *See, e.g.*, U.S. DEP'T OF JUSTICE, THE NATIONAL STRATEGY FOR CHILD EXPLOITATION AND INTERDICTION 16-17 (2016), https://www.justice.gov/psc/file/842411/download [https://perma.cc/6MZH-DKUN] (last visited June 7, 2019).

9. *See* Joshuah Bearman & Tomer Hanuka, *The Rise and Fall of Silk Road: Part I*, WIRED.COM, https://www.wired.com/2015/04/silk-road-1/ [https://perma.cc/7L85-MM86] (last visited June 7, 2019) (discussing the "take down" of The Dark Web drug bazar); Joshuah Bearman & Tomer Hanuka, *The Rise & Fall of Silk Road: Part II*, WIRED.COM, https://www.wired.com/2015/05/silk-road-2 [https://perma.cc/LXR8-7W75] (last visited June 7, 2019); *Darknet Market Archives*, GWERN, https://www.gwern.net/DNM-archives [https://perma.cc/8MBN-DD6T] (last visited June 7, 2019).

10. *See Hacker Jailed for Selling Asda and Uber Customers' Data on Dark Web*, THE GUARDIAN (May 25, 2018, 10:08 PM), https://www.theguardian.com/technology/2018/may/25/hacker-jailed-for-selling-asda-and-uber-customers-data-on-dark-web [https://perma.cc/7LVL-MHNY]; *see also* John Brandon, *Your Online Identity Sells for Exactly $1,170 on the Dark Web—Here's How to Block the Sale*, FOX NEWS (Mar. 28, 2018), http://www.foxnews.com/tech/2018/03/28/your-online-identity-sells-for-exactly-1170-on-dark-web-heres-how-to-block-sale.html [https://perma.cc/849U-AXTL] (discussing how stolen identify information is sold on The Dark Web).

11. *CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders*, CTR FOR STRATEGIC & INT'L STUDIES (June 6, 2016), https://www.csis.org/events/ccips-csis-cybercrime-symposium-2016 [https://perma.cc/56EJ-69DQ].

12. *Id.*

13. *Id.*

14. Ahmed Ghappour, *Searching Places Unknown: Law Enforcement Jurisdiction on the Dark Web*, 69 STAN. L. REV. 1075, 1082 (2017).

15. United States v. Kahler, 236 F. Supp. 3d 1009, 1021 (E.D. Mich. 2017).

protect confidential government information.[16] The literature is not clear on how this confidential project led to Tor being the popular access route to The Dark Web. Interestingly, the Tor website is quite docile looking and hardly would lead a viewer to suspect that it is the pipeline to so much that is evil in the world.[17] The key piece of data hidden by Tor is the unique "IP address" of each computer accessing the Internet through that browser.[18]

C. Virtual Currencies Enable The Dark Web

In less than a decade, virtual currencies are proving to be a unique payment system challenge for law enforcement, financial regulatory authorities worldwide, and the investment community.[19] The rapid introduction and development of blockchain, which enables Bitcoin's crypto-foundation, is overwhelming the ability of law enforcement and the regulators to keep pace.[20] The U.S. Department of the Treasury's Financial Crimes Enforcement Network (FinCEN) states that virtual currency consists of "those currencies that operate like a currency in some environments, but does not have legal tender status in any jurisdiction."[21] The Financial Action Task Force provides a more comprehensive definition:

> a digital representation of value that can be digitally traded and functions as: (1) a medium of exchange; and/or (2) a unit of account; and/or (3) a store of value, but does not have legal tender status (i.e., when tendered to a creditor, is a valid and legal offer of payment) in any jurisdiction. It is not issued or guaranteed by any jurisdiction, and fulfills the above

16. Kurt C. Widenhouse, *Playpen, the NIT, and Rule 41(b): Electronic "Searches" for Those Who Do Not Wish to be Found*, 13 J. BUS. & TECH. L. 143 (2017).

17. TORPROJECT.ORG, https://www.torproject.org/about/sponsors.html.en [https://perma.cc/3S77-YWUJ] (last visited June 7, 2019).

18. Widenhouse, supra note 16; *see IP Address*, MERRIAM-WEBSTER DICTIONARY, https://www.merriam-webster.com/dictionary/IP%20address [https://perma.cc/VQ4X-WSYQ] (last visited June 7, 2019).

19. *See* Lawrence J. Trautman, *Bitcoin, Virtual Currencies and the Struggle of Law and Regulation to Keep Pace,* 102 MARQ. L. REV. 447 (2018); Lawrence J. Trautman & Alvin C. Harrell, *Bitcoin versus Regulated Payment Systems: What Gives?,* 38 Cardozo L. Rev. 1041 (2017).

20. *Id.*

21. *Beyond Silk Road: Potential Risks, Threats, and Promises of Virtual Currencies: Hearing Before the Comm. on Homeland Sec. & Governmental Affairs*, 113th Cong., 73 n.4 (Nov. 18, 2013) (prepared testimony of Edward Lowery III, Special Agent in Charge, Criminal Investigative Division, U.S. Secret Service) *citing* Dep't of Treasury Fin. Crimes Enf't Network, Guidance FIN-2013-G0001*, Application of FinCENS's Regulations to Persons Administrating, Exchanging, or Using Virtual Currencies* (Mar. 18, 2013)).

> functions only by agreement within the community of users of the virtual currency.[22]

As of August 31, 2018, Coinmarketcap.com lists 1,910 different cryptocurrencies, having a total market capitalization of approximately $229.8 billion.[23]

The advantage of the use of Bitcoins and other virtual currencies in criminal enterprises is obvious.[24] Just a few of the illicit activities known to involve payment with Bitcoin include: "illicit drugs;[25] sales of armaments, often involving terrorist organizations;[26] money laundering;[27] marketplace for assassins;[28] child exploitation;[29] corporate espionage;[30] fake IDs and passports;[31] sexual exploitation;[32] high yield investment schemes;[33] stolen credit cards;[34] and many other activities where masking the identities of parties to the transaction is involved.[35] Ransomware attacks are discussed in a separate subsection below.[36] Carnegie Mellon researchers and those based in Delft Technical University in the Netherlands, collected data between 2011 and 2017 from anonymous major online marketplaces.[37] The researchers reported

22. FIN. ACTION TASK FORCE, Virtual Currencies, Key Definitions and Potential AML/CFT Risks, (June 2014), https://www.fatf-gafi.org/media/fatf/documents/reports/Virtual-currency-key-definitions-and-potential-aml-cft-risks.pdf [https://perma.cc/DJA6-93QH].

23. *All Cryptocurrencies,* COINMARKETCAP (Aug. 31, 2018), https://coinmarketcap.com/all/views/all/ [https://perma.cc/KL33-7BPV].

24. *See* Dan Awrey & Kristin van Zwieten, *The Shadow Payment System*, 43 IOWA J. CORP. L., 775 (2018).

25. Lawrence J. Trautman, *Virtual Currencies; Bitcoin & What Now After Liberty Reserve, Silk Road, and Mt. Gox?,* 20 RICH. J. L. & TECH. 13, 12-13 (2014).

26. *See also* Alan Brill & Lonnie Keene, *Cryptocurrencies: The Next Generation of Terrorist Financing?,* 6 DEFENCE AGAINST TERRORISM REV. 7 (2014), https://ssrn.com/abstract=2814914 [https://perma.cc/U6E8-JKNY].

27. *Id. See also* Danton Bryans, *Bitcoin and Money Laundering: Mining for an Effective Solution,* 89 IND. L.J. 441(2014); Allison Caffarone & Meg Holzer, *'Ev'ry American Experiment Sets a Precedent': Why One Florida State Court's Bitcoin Opinion is Everyone's Business,* 16 HOFSTRA L.J. INT'L BUS. & L., https://ssrn.com/abstract=2897727 [https://perma.cc/C2F2-7HHV]; Catherine Martin Christopher, *Whack-a-Mole: Why Prosecuting Digital Currency Exchanges Won't Stop Online Laundering,* 18 LEWIS & CLARK L. REV. 1 (2014), https://ssrn.com/abstract=2312787 [https://perma.cc/8YN7-ZHAG].

28. Trautman, *supra* note 25, at 8-9.

29. *Id.* at 9-11.

30. *Id.* at 11-12.

31. *Id.* at 13-14.

32. *Id.* at 14.

33. *Id.* at 14.

34. *Id.* at 15.

35. *Id.* at 8.

36. *See infra* Section II.D.

37. *After the Breach: The Monetization and Illicit Use of Stolen Data: Hearing Before the Subcomm. On Terrorism & Illicit Fin., Comm. On Fin. Services, U.S. House of Representatives* 7 (2018) (statement of Nicolas Christin, Assoc. Research Professor, Carnegie Mellon Univ.).

that roughly 25% of the observed activities on The Dark Web were fraudulent financial schemes of some kind.[38]

Transnational criminal organizations (TCOs) constitute "a significant and growing threat to the United States financial system and [its] national security."[39] The House Terrorism and Illicit Finance Subcommittee conducted hearings on "Exploring the Financial Nexus of Terrorism, Drug Trafficking, and Organized Crime" on March 20, 2018.[40] The Financial Services Committee staff writing:

> These organizations have an estimated value of $3.6 to $4.8 trillion, or seven percent of global Gross Domestic Product, and result in $130 billion in lost revenue annually to the private sector. TCOs should be regarded as a national security threat that is undermining U.S. government efforts to combat illegal drugs, arms, human trafficking, terrorism, and other crimes to include money laundering, cybercrimes, fraud, and corruption. Given the profit potential, terrorist and insurgent groups have been steadily incorporating criminal activities into their business models, thus blurring the line between TCOs and terrorist organizations…[41]

D. Cybercrimes and The Dark Web

Due to the volume of material on cybercrimes, a comprehensive update is beyond the scope of this article. This section will present a brief overview and examples of the current level and nature of cyber threats. In his August 21, 2018 testimony before the Senate Judiciary's Subcommittee on Crime and Terrorism's Hearing on Cyber Threats to Our National Critical Infrastructure, Associate Deputy Attorney General Sujit Raman states:

> Cyber threats to critical infrastructure deserve particular attention, because our Nation's critical infrastructure provides the essential services that underpin American society and serves as the backbone of our economy, security, and health systems. Critical infrastructure includes the financial services sector, the electrical grid, dams, electoral systems, and over a dozen other sectors of society. Those assets, systems, and networks are considered so vital to the United States that their incapacitation or destruction would have a debilitating effect on our national security, national economic security, or our national public health or safety —

38. *Id.*
39. H.R. REP. NO. 115-1122, at 190 (2019).
40. *Id.*
41. *Id.*

> or any combination thereof. Our adversaries seek to identify and exploit vulnerabilities in the sophisticated computer networks that these sectors employ.[42]

Cyber threats and attacks from nation states continue as private entities and government agencies act to stem the tide.[43] When compared to highly controlled economies or nation states with authoritarian governmental control, one of the costs associated with having an open and free society is that it is more vulnerable to attacks from actors who can hide their activities in The Dark Web.[44] The U.S. Computer Emergency Readiness Team reported that, "[s]ince at least March 2016, Russian government cyber actors (hereafter referred to as "threat actors") targeted government entities and multiple U.S. critical infrastructure sectors, including the energy, nuclear, commercial facilities, water, aviation, and critical manufacturing sectors."[45]

In addition to Russia, considerable malicious cyber activity is attributed by the U.S. government during 2018 to other nation state actors including Iran and North Korea. Accordingly, the U.S. Department of Justice (DOJ) states:

> We know that the Iranian government has targeted our critical infrastructure, specifically our financial sector, with cyberattacks. In response, in March 2016, a federal grand jury indicted seven Iranian hackers belonging to two companies that worked for Iran's Islamic Revolutionary Guard Corps for their role in Distributed Denial of Service ("DDoS") attacks targeting the public-facing websites of nearly fifty U.S. banks.
>
> To take another example — this one involving North Korea — in May 2018, the FBI and DHS issued a technical alert notifying the public about the FBI's high confidence that malicious North Korean government cyber actors have been using malware since at least 2009 "to target multiple victims

42. Sujit Raman, Assoc. Deputy Attorney, Opening Statement to the Senate Comm. on Crime and Terrorism's Hearing on Cyber Threats to Our Nation's Critical Infrastructure (Aug. 21, 2018).

43. *See generally* Lawrence J. Trautman & Peter C. Ormerod, *Corporate Directors' and Officers' Cybersecurity Standard of Care: The Yahoo Data Breach,* 66 AM. U. L. REV. 1231 (2017); Lawrence J. Trautman, *Is Cyberattack The Next Pearl Harbor?,* 18 N.C. J. L. & TECH. 233 (2016).

44. *See* Michael Chertoff & Tobby Simon, *The Impact of the Dark Web on Internet Governance and Cyber Security*, 6 Global Comm. on Internet Governance 1, 4 (2015)*; see also* Trautman, *supra* note 25.

45. *Alert (TA18-074A) Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors*, UNITED STATES DEPARTMENT OF HOMELAND SECURITY CISA, (Mar. 16, 2018) https://www.us-cert.gov/ncas/alerts/TA18-074A [https://perma.cc/HY2Y-GSHG].

> globally and in the United States," across various sectors — including critical infrastructure sectors.[46]

The notoriety of The Dark Web is attributed to what is found and sold there. Recent television advertising for identity theft services even offer to scan that part of the Internet to see if a customer's personal information is up for sale there.[47] Much of what the general public knows about The Dark Web comes from reports on high-profile enforcement actions.[48] Perhaps the two best known law enforcement actions were against "The Silk Road" and "Playpen." Both are discussed below with additional examples.

1. The Silk Road

The Silk Road was reported to be a site primarily for the purchase of illegal drugs.[49] The FBI carefully monitored the site, along with several other law enforcement agencies, but it was unable to trace it back to a person or location.[50] However, a mistake in the system allowed the FBI to trace the system back to its server in Iceland and from there, to San Francisco and the mastermind behind it, Ross Ulbricht.[51] He also went by the moniker "Dread Pirate Roberts," adding to the colorful presentation of the case against him.[52] Ulbricht was sentenced to life in prison for his role in the drug trade.[53] After a federal appeals court upheld his conviction and sentencing, Ulbricht's attorneys filed an appeal with the U.S. Supreme Court.[54] Both Ulbricht and the United States filed briefs and replies and there were *amicus* briefs filed as well.[55] However, the Supreme Court denied certiorari in June 2018.[56] The

46. *Id.*

47. *See* Tara Siegel Bernard, *The Post-Equifax Marketing Push: Identity Protection Services,* N.Y. TIMES (Oct. 25, 2017), https://www.nytimes.com/2017/10/25/your-money/identity-protection-equifax.html [https://perma.cc/8V7P-PGZ2].

48. *See, e.g.* Nathaniel Popper, *Dark Web Drug Sellers Dodge Police Crackdowns*, N.Y. TIMES (June 11, 2019), https://www.nytimes.com/2019/06/11/technology/online-dark-web-drug-markets.html [https://perma.cc/PHY9-CWCH].

49. *See* Bearman & Hanuka, *supra* note 9, Part I.

50. *See* Bearman & Hanuka, *supra* note 9, Part II.

51. *Id.*

52. *Id.*

53. *See* Benjamin Weiser, *Ross Ulbricht, Creator of Silk Road Website, Is Sentenced to Life in Prison,* N.Y. TIMES (May 29, 2015), https://www.nytimes.com/2015/05/30/nyregion/ross-ulbricht-creator-of-silk-road-website-is-sentenced-to-life-in-prison.html [https://perma.cc/M6F2-U9EW].

54. *See generally* Andrew Blake, *Silk Road Administrator Appeals Case Before Supreme Court*, WASH. TIMES (Dec. 28, 2017), https://www.washingtontimes.com/news/2017/dec/28/ross-ulbricht-silk-road-administrator-appeals-case/ [https://perma.cc/YY8S-9FWB].

55. *Ulbricht v. United States*, SCOTUSBLOG, http://www.scotusblog.com/case-files/cases/ulbricht-v-united-states/ [https://perma.cc/E9FG-S3CH] (last visited June 7, 2019).

56. *Id.*

high court's decision not to review the case would appear to be a tacit approval of the procedure used by the FBI to locate Mr. Ulbricht.

2. Playpen, FBI, and Child Pornography

Playpen was a site for the sale and distribution of child pornography.[57] In a bizarre twist to the story, the FBI seized the site in 2015, but operated the site for two weeks and used the NIT in order to identify and prosecute customers of the site.[58] Ultimately, the FBI's use of the NIT hacking tool led to charges against 186 persons.[59] However, because the federal judge who authorized the warrant was in Virginia, the server was in North Carolina, and the pedophiles were in various states, the issue of the propriety of the searches has been raised.[60]

Illegal distribution of weapons on The Dark Web has also been documented by the arrest and prosecution of Michael Albert Focia.[61] The high-profile federal prosecution of Mr. Focia is one of the few cases involving The Dark Web to reach federal appellate courts, other than the Ulbricht case referenced above.[62] Focia operated the site "Black Market Reloaded."[63] He was convicted of selling weapons without a license through the site.[64] Focia challenged his prosecution mostly on procedural grounds, and so far, has failed at both the federal district court and appeals level.[65] A 2015 white paper detailing the identity and financial products for sale on The Dark Web included color photos of passports from several countries, a variety of VISA cards with various dollar limits, and information for PayPal and other accounts.[66] Purchasers also had the opportunity to purchase counterfeit money and even former President Bill Clinton's identity.[67]

57. Benson Varghese, *How The FBI Ended Up Running A Child Porn Website*, LAW360 (Sept. 8, 2016), https://www.law360.com/articles/837195/how-the-fbi-ended-up-running-a-child-porn-website [https://perma.cc/CJ8X-56YU].

58. *Id.*

59. *Id.*

60. *Id.*

61. *See* United States v. Focia, 869 F.3d 1269 (11th Cir. 2017).

62. See *Ulbricht v. United States*, *supra* note 55.

63. *Focia,* 869 F.3d at 1274.

64. *Id.* at 1277.

65. *See id.* at 1277-88; s*ee also* Focia v. United States, 139 S. Ct. 846 (2019) (petition for writ of certiorari denied).

66. Marco Balduzzi & Vincenzo Ciancaglini, *Cybercrime in the Deep Web*, BLACK HAT EUROPE (2015), 27-30, https://www.blackhat.com/docs/eu-15/materials/eu-p15-Balduzzi-Cybercrmine-In-The-Deep-Web.pdf [https://perma.cc/AS3A-VCPR] (last visited Sept. 28, 2019).

67. *Id.* at 28; Vincenzo Ciancaglini et al., *Below the Surface: Exploring the Deep Web*, TREND MICRO, at 30, https://documents.trendmicro.com/assets/wp/wp_below_the_surface.pdf [https://perma.cc/T7RK-YAHH] (last visited Sept. 28, 2019).

Also available on The Dark Web are opportunities to purchase malware. This type of software is often used to threaten or to put in place ransom demands using command and control software.[68] Because the host address is not within the normal realm of the Internet, it is more difficult to track the source of the malware and may lead computer users to open the dangerous software since there is not a clear or easily traceable IP address.[69] A reported trend in The Dark Web is the operation of sites for short periods of time during which millions of dollars in Bitcoins are accumulated, and then the site is shut down and the operators abscond with the proceeds.[70] One such "exit scam" landed the operator in police custody and under charges where he could face a dozen years behind bars.[71]

3. Silk Road 2.0

Following the successful takedown of the operations known as Silk Road,[72] European (Europol's European Cybercrime Centre and Eurojust)[73] and U.S. authorities took further joint action against numerous dark market websites and the site known as "Silk Road 2.0," which had been created one month after seizure of Silk Road during October 2013.[74] The July 2018 Report of the Attorney General's Cyber Digital Task Force states, "[a]s with Silk Road, the Department used civil forfeiture authorities to seize control [of] over 400 Tor website addresses known as '.onion' addresses, as well as the servers hosting them. Administrators associated with these Dark Web markets were criminally prosecuted."[75] As was the case with the website known as Silk Road, dozens of dark market websites and Silk Road 2.0 engaged in activities including, "facilitating the sale of an astonishing range of illegal goods and services on hidden servers within the Tor network, including

68. Ciancaglini et al., *supra* note 67.

69. *Id.*

70. Benjamin Brown, *2016 State of the Dark Web*, AKAMAI THREAT ADVISORY, at 4, https://www.akamai.com/cn/zh/multimedia/documents/state-of-the-internet/akamai-2016-state-of-the-dark-web.pdf [https://perma.cc/MA3U-ZGTZ] (last visited Sept. 29, 2019).

71. *Id.*

72. *See* Trautman, *supra* note 25, at 99.

73. *See* Press Release, U.S. Attorney, Southern District of New York, *Dozens of Online 'Dark Markets' Seized Pursuant to Forfeiture Complaint Filed in Manhattan Federal Court in Conjunction with the Arrest of the Operator of Silk Road 2.0*, Federal Bureau of Investigation (Nov. 7, 2014), https://www.fbi.gov/contact-us/field-offices/newyork/news/press-releases/dozens-of-online-dark-markets-seized-pursuant-to-forfeiture-complaint-filed-in-manhattan-federal-court-in-conjunction-with-the-arrest-of-the-operator-of-silk-road-2.0 [https://perma.cc/N4UY-UEKC].

74. *See* REPORT OF THE ATTORNEY GENERAL'S CYBER DIGITAL TASK FORCE, DOJ 138 (July 2, 2018), https://www.justice.gov/ag/page/file/1076696/download [https://perma.cc/78PX-VZTF].

75. *Id.*

weapons, drugs, murder-for-hire services, stolen identification data, money laundering, hacking services, and others."[76] According to Manhattan U.S. Attorney Preet Bharara:

> As illegal activity online becomes more prevalent, criminals can no longer expect that they can hide in the shadows of the 'dark web.' We shut down the original Silk Road website and now we have shut down its replacement, as well as multiple other 'dark market' sites allegedly offering all manner of illicit goods and services, from firearms to computer hacking. In coordination with domestic and international law enforcement agencies, we will continue to seize websites that promote illegal and harmful activities, and prosecute those who create and operate them.[77]

4. Darkode

The 2015 charges brought against computer hacking forum, Darkode, illustrates the difficulty of investigating and prosecuting global dark web criminal activities. Darkode represents, "a coordinated effort by a coalition of law enforcement authorities from 20 nations to charge, arrest or search 70 Darkode members and associates around the world."[78] Jurisdictions involved in this coordinated effort include: "Australia, Bosnia and Herzegovina, Brazil, Canada, Colombia, Costa Rica, Cyprus, Croatia, Denmark, Finland, Germany, Israel, Latvia, Macedonia, Nigeria, Romania, Serbia, Sweden, the United Kingdom and the United States… [constituting] the largest coordinated international law enforcement effort ever directed at an online cyber-criminal forum."[79] U.S. Attorney David J. Hickton of the Western District of Pennsylvania observes, "[o]f the roughly 800 criminal internet forums worldwide, Darkode represented one of the gravest threats to the integrity of data on computers in the United States and around the world and was the most sophisticated English-speaking forum for criminal computer hackers in the world."[80] In addition, U.S. Attorney Hickton states, "Through this operation, we have dismantled a cyber hornets' nest of criminal hackers which was believed by many, including the hackers themselves, to be impenetrable."[81] The DOJ reports:

76. *Id.* (citing Press Release, *'Dark Markets,' supra* note 73).
77. Press Release, *'Dark Markets,' supra* note 73.
78. Press Release, DOJ, *Major Computer Hacking Forum Dismantled* (July 15, 2015), https://www.justice.gov/opa/pr/major-computer-hacking-forum-dismantled [https://perma.cc/3XRS-QB9D].
79. *Id.*
80. *Id.*
81. *Id.*

> As alleged in the charging documents, Darkode was an online, password-protected forum in which hackers and other cyber-criminals convened to buy, sell, trade and share information, ideas, and tools to facilitate unlawful intrusions on others' computers and electronic devices. Before becoming a member of Darkode, prospective members were allegedly vetted through a process in which an existing member invited a prospective member to the forum for the purpose of presenting the skills or products that he or she could bring to the group. Darkode members allegedly used each other's skills and products to infect computers and electronic devices of victims around the world with malware and, thereby gain access to, and control over, those devices.[82]

5. AlphaBay & Hansa

On July 20, 2017, the DOJ announced seizure of AlphaBay, at the time "the largest criminal marketplace on the Internet . . . which operated globally for over two years on the dark web and was used to sell deadly illegal drugs, stolen and fraudulent identification documents and access devices, counterfeit goods, malware and other computer hacking tools, firearms, and toxic chemicals."[83] AlphaBay's operator was Alexandre Cazes, a Canadian citizen who was captured in Thailand.[84] He later committed suicide before he could be extradited to the United States.[85] Cazes and his wife's assets were located throughout the world and included luxury vehicles, residences, and even a hotel in Thailand.[86] The FBI and the U.S. Drug Enforcement Administration (DEA) also seized cryptocurencies with a market value in the millions of dollars.[87] The United States led the coordinated effort to take down AlphaBay and involved law enforcement authorities in Thailand, the Netherlands, Lithuania, Canada, the United Kingdom, and France, as well as Europol.[88] Prior to the take down, an AlphaBay staff member made a claim that the site "serviced over 200,000 users and 40,000 vendors."[89]

"AlphaBay operated as a hidden service on the 'Tor' network, and utilized cryptocurrencies including Bitcoin, Monero and Ethereum in order to hide the locations of its underlying servers

82. *Id.*
83. *See* Press Release, *AlphaBay, the Largest Online 'Dark Market,' Shut Down*, DEP'T OF JUST. (July 20, 2017), https://www.justice.gov/opa/pr/alphabay-largest-online-dark-market-shut-down [https://perma.cc/J832-MQQD].
84. *Id.*
85. *Id.*
86. *Id.*
87. *Id.*
88. *Id.*
89. *Id.*

and the identities of its administrators, moderators, and users."[90] Of great concern, based on their investigation, "authorities believe the site was also used to launder hundreds of millions of dollars deriving from illegal transactions on the website."[91] AlphaBay's operations are also implicated in a number of deaths according to the DOJ:

> According to a complaint affidavit filed in the District of South Carolina against Theodore Vitality Khleborod and Ana Milena Barrero, an investigation into an overdose death on February 16, in Portland, Oregon, involving U-47700, a synthetic opioid, revealed that the drugs were purchased on AlphaBay from Khelborod and Barrero. According to another complaint affidavit filed in the Middle District of Florida against Jeremy Achey, an investigation into a fentanyl overdose death in Orange County, Florida, on February 27, revealed that the lethal substance was purchased on AlphaBay from Achey.[92]

6. Operation Darkness Falls

Just one of many examples of dark net criminal activity is represented by the August 22, 2018 announcement by the FBI, DOJ, DEA, U.S. Postal Inspection Service (USPIS), and Immigration and Customs Enforcement's (ICE) Homeland Security Investigations of "several arrests, charges and guilty pleas as a result of "Operation Darkness Falls," a joint operation targeting people and organizations that sell fentanyl and other drugs over the dark net… [including] the most prolific dark net fentanyl vendor in the United States and the fourth most prolific in the world – MH4Life."[93]

Court documents disclosed that Matthew and Holly Roberts of San Antonio, TX, were charged earlier in 2018 with multiple crimes related to their operation of multiple marketplace accounts, including the deadly MH4Life.[94] They utilized dark net websites including Dream Market, Silk Road, AlphaBay, Darknet Heroes League, and Nucleus.[95] MH4Life was alleged to have been a

90. *Id.*
91. *Id.*
92. *Id.*
93. *Operation Darkness Falls Results in Arrest of One of the Most Prolific Dark Net Fentanyl Vendors in the World,* DEP'T OF JUST. (Aug. 22, 2018), https://www.justice.gov/opa/pr/operation-darkness-falls-results-arrest-one-most-prolific-dark-net-fentanyl-vendors-world [https://perma.cc/DU2R-DTWZ].
94. *Id.*
95. *Id.*

location for the sale of illegal narcotics, and the prosecutors allege the site hosted a record number of fentanyl sales.[96]

E. Ransomware

In the discussion above, this article reviews a variety of sites found on The Dark Web where persons can go to buy and sell a variety of items, most of them harmful to themselves or others. However for most of what is for sale, the buyer initiated those purchases. In the case of ransomware, unsuspecting computer users around the world are being held hostage by the most pernicious of devices.

A recent white paper by Trautman and Ormerod provides more details on the "Wannacry" ransomware attacks and others.[97] This subsection will summarize some of the key issues related to the growing frequency, cost, disruption, and significance of this type of criminal activity. Deputy Attorney General Rod Rosenstein reported "that the monetary costs of global annual cybercrime will double from $3 trillion in 2015 to $6 trillion in 2021. Those numbers are staggering; and recent events demonstrate why we need to work together to address the growing threat."[98] FBI director Christopher Wray stated:

> [T]he frequency and impact of cyber-attacks on our nation's private sector and government networks have increased dramatically in the past decade and are expected to continue to grow. We continue to see an increase in the scale and scope of reporting on malicious cyber activity that can be measured by the amount of corporate data stolen or deleted, personally identifiable information compromised, or remediation costs incurred by U.S. victims. Within the FBI, we are focused on the most dangerous malicious cyber activity: high-level intrusions by state-sponsored hackers and global organized crime syndicates, as well as other technically sophisticated attacks.[99]

96. *Id.*

97. *See* Lawrence J. Trautman & Peter C. Ormerod, *Wannacry, Ransomware, and the Emerging Threat to Corporations*, 86 TENN. L. REV. 503, 522-30 (2019); *see also* Lawrence J. Trautman & Peter C. Ormerod, *Industrial Cyber Vulnerabilities: Lessons from Stuxnet and the Internet of Things*, 72 U. MIAMI L. REV. 761 (2018).

98. U.S. Dep't of Justice, *Deputy Attorney General Rosenstein Delivers Remarks at the 2017 North American Int'l Cyber Summit* (Oct. 30, 2017), https://www.justice.gov/opa/speech/deputy-attorney-general-rosenstein-delivers-remarks-2017-north-american-international [https://perma.cc/ZSE8-3MUV].

99. *Current Threats to the Homeland: Hearing Before the S. Homeland Sec. & Gov't Affairs Comm.*, 115th Cong. (2017) (statement of Christopher Wray, Dir., Fed. Bureau of Investigation); *Threats to the Homeland: Hearing Before the S. Homeland Sec. & Gov't*

Any computer user, from a lone user in Peoria to large organizations engaged in healthcare or critical infrastructure, like power plants and police forces, can be impacted by ransomware. This is an "an insidious type of malware that encrypts, or locks, valuable digital files and demands a ransom to release them."[100] In large organizations, it only takes a single user to make a mistake and click on the wrong email link or attachment to give the intruder access to install malware that can lock a system until a cyberkey is purchased with cybercurrency.[101]

Of special concern due to the obvious impact on human life are ransomware attacks on healthcare facilities. According to Professor Deborah Farringer, "[w]hile hackers and data breaches are not new in the healthcare context, ransomware attacks are unique in the way they have a direct and immediate impact on the actual provision of care to patients and present a very real threat to patient safety."[102] She also noted that risks could occur to hospitals and healthcare facilities, electronic health records, and computer systems.[103] This risk has actually accelerated as hospitals and healthcare facilities continue to move to all electronic records as mandated by the Health Insurance Portability and Accountability Act of 1996 (HIPAA).[104]

Becker Hospital Review reported twelve ransomware attacks against hospitals during 2016 alone, ranging from a small hospital in rural Texas to larger hospitals around the United States, as well as Canada and Germany.[105] A detailed example was the 2016 ransomware attack on MedStar Health, a non-profit group of ten hospitals in the Washington, D.C. area.[106] The hackers demanded Bitcoins equivalent to $19,000.[107] The news report indicated that

Affairs Comm., 115th Cong. (statement of Christopher Wray, Dir., Fed. Bureau of Investigation)

100. *Cyber Crime: Key Priorities, Ransomware*, FED. BUREAU OF INVESTIGATION, https://www.fbi.gov/investigate/cyber [https://perma.cc/J7HC-Y83Y] (last visited Oct. 11, 2019).

101. *Id.*

102. Deborah R. Farringer, *Send Us the Bitcoin or Patients Will Die: Addressing the Risks of Ransomware Attacks on Hospitals,* 40 SEATTLE U. L. REV. 937, 939-40 (2017) (citations omitted).

103. *Id.* at 940.

104. Health Insurance Portability and Accountability Act of 1996, Pub. L. 104-191,110 Stat. 1936 (1996); *see also* Farringer, *supra* note 102, at 943-51 (discussing in depth the evolution and adoption of HIPAA and related laws as they pertain to electronic health records).

105. *12 Healthcare Ransomware Attacks of 2016*, BECKER'S HOSP. REV. (Dec. 29, 2016), https://www.beckershospitalreview.com/healthcare-information-technology/12-healthcare-ransomware-attacks-of-2016.html [https://perma.cc/J6JT-EE8X].

106. *MedStar Recovering from Computer Virus: 7 Things to Know,* BECKER'S HOSP. REV. (Mar. 30, 2016), https://www.beckershospitalreview.com/healthcare-information-technology/medstar-recovering-from-computer-virus-7-things-to-know.html [https://perma.cc/8JH7-MWVS].

107. *Id.*

the hospital was forced to operate without computers and rely on paper patient records to avoid using their apparently infected computer system.[108]

Municipalities, educational and other public institutions have also proven to be an attractive target for ransomware criminals.[109] For example, the St. Louis Public Library was reportedly the victim of a $25,000 ransom demand during 2017.[110] "Local governments are forced to spend money on frantic efforts to recover data, system upgrades, cybersecurity insurance and, in some cases, to pay their online extortionists if they can't restore files some other way."[111]

Private corporations are increasingly the targets of ransomware attacks, although some corporations are hiding the existence of such attacks to avoid damage to their reputations and avoid alarming their customers and clients.[112] Deputy U.S. Attorney General Rod Rosenstein warns, "Cyber criminals know that a company's lifeblood is contained in its networks and the information flowing through those systems. The last few years have witnessed a significant increase in criminals using ransomware."[113] For many years, extortion schemes have been used by transnational organized crime syndicates.[114] This new technology vulnerability is added to the long list of crises that face corporate officers, directors, and managers.[115]

The increased use of multiple electronic devices by each corporate employee, often referred to as Bring-Your-Own-Device

108. John Woodrow Cox, *MedStar Health Turns Away Patients After Likely Ransomware Cyberattack*, WASH. POST (Mar. 29, 2016), https://www.washingtonpost.com/local/medstar-health-turns-away-patients-one-day-after-cyberattack-on-its-computers/2016/03/29/252626ae-f5bc-11e5-a3ce-f06b5ba21f33_story.html [https://perma.cc/X3FU-UGJW] (search "MedStar health ransomware")

109. *Id.*

110. Jon Kamp & Scott Clavert, *Ransom Demands and Frozen Computers: Hackers Hit Towns Across the U.S.*, WALL ST. J. (June 24, 2018), https://www.wsj.com/articles/ransom-demands-and-frozen-computers-hackers-hit-towns-across-the-u-s-1529838001 [https://perma.cc/6VVF-XE6K].

111. *Id.*

112. Eamon Javers, *Cyberattacks: Why Companies Keep Quiet*, CNBC (Feb. 25, 2013) https://www.cnbc.com/id/100491610 [https://perma.cc/G6KZ-5N9H].

113. U.S. Dep't of Justice, *supra* note 98.

114. *Transnational Organized Crime*, NAT'L SEC. COUNCIL, https://obamawhitehouse.archives.gov/administration/eop/nsc/transnational-crime/threat [https://perma.cc/WY6K-5XKG] (last visited Oct. 11, 2019).

115. *See generally* Lawrence J. Trautman, *The Board's Responsibility for Crisis Governance,* 13 HASTINGS BUS. L. J. 275 (2017) (discussing the threat that natural disasters pose to corporations); Lawrence J. Trautman & George Michaely, *The SEC & The Internet: Regulating the Web of Deceit,* 68 CONSUMER FIN. L. Q.R. 262 (2014) (discussing regulation of the internet and electronic transactions); Lawrence J. Trautman, *Who Qualifies as an Audit Committee Financial Expert Under SEC Regulations and NYSE Rules?,* 11 DEPAUL BUS. & COMM. L. J. 205 (2013) (discussing the need for cybersecurity expertise represented on corporate boards).

(BYOD), has resulted in increased cyber threats to corporations.[116] Numerous employee personal digital devices, such as personal laptops, smart phones, and iPads, when interconnected with corporate data, expose corporate data systems to the vulnerabilities of employee devices.[117] As Bruce Schneier writes:

> Everything is becoming a computer. Your microwave is a computer that makes things hot. Your refrigerator is a computer that keeps things cold. Your car and television, the traffic lights and signals in your city and our national power grid are all computers. This is the much-hyped Internet of Things (IoT). It's coming, and it's coming faster than you might think. And as these devices connect to the Internet, they become vulnerable to ransomware and other computer threats.[118]

F. Positive Uses for the Dark Web

Some may ask if there is so much that is evil on The Dark Web, is it legal to access it and to use Tor and similar browsers? "Yes – such dedicated browsers are used by the military, police, journalists and whistleblowers to maintain their privacy online."[119] First, the anonymous nature of The Dark Web affords whistleblowers the chance to report wrongdoing at their place of employment without risking retaliation.[120] Second, in a similar vein, reporters can use this route while gathering evidence to guarantee privacy to sources that would not otherwise come forward.[121] Third, not frequently mentioned is the fact that many computer users are tired of using commercial web browsers and then being bombarded with emails

116. *See* Pedro Pavón, *Risky Business: "Bring-Your-Own-Device" and Your Company*, AM. BAR ASS'N (Sept. 30, 2013), https://www.americanbar.org/groups/business_law/publications/blt/2013/09/01_pavon/ [https://perma.cc/TM39-VKXP].

117. *Id.*

118. Bruce Schneier, *The Future of Ransomware*, SCHNEIER ON SECURITY (May 23, 2017), https://www.schneier.com/blog/archives/2017/05/the_future_of_r.html [https://perma.cc/73YV-C3S4]; *see also* Lawrence J. Trautman, Mason Molesky, Mohammed T. Hussein & Louis Ngamassi, *Governance of The Internet of Things (IoT): A Primer,* (unpublished manuscript), http://ssrn.com/abstract=3443973 [https://perma.cc/WQY9-Y7QF].

119. Anthony Lieu, *Is It Legal to Access the Deep Web and use Tor?* LEGALVISION.COM (July 10, 2019), https://legalvision.com.au/is-it-legal-to-access-the-deep-web-and-use-tor/ [https://perma.cc/6KZP-F69N].

120. *See* Andy Greenberg, *A Guide to the Dark Webb's Lighter Side,* WIRED (Sept. 1, 2015), https://www.wired.com/2015/09/guide-dark-webs-lighter-side/ [https://perma.cc/F2YM-6XY2].

121. *See CCIPS-CSIS Cybercrime Symposium 2016: Cooperation and Electronic Evidence Gathering Across Borders*, CTR. FOR STRATEGIC & INT'L STUDIES (Jun. 6, 2016), https://www.csis.org/events/ccips-csis-cybercrime-symposium-2016 [https://perma.cc/G662-NL7S].

advertising the products for which they most recently searched, from hotels to household supplies to automobiles.[122]

There is also growing concern that major search engines like Google are censoring some of the search results on the Internet. Elected officials from both major political parties have expressed concern about possible censorship and reduced access to such search engines.[123] Persons seeking uncensored news may resort to unconventional sources like The Dark Web.

II. COURT RULINGS AND THE DARK WEB

The current legal arena is a confusing mix of decisions at this time. Federal courts have struggled to apply constitutional provisions in cases that concern digital privacy.[124] There is no U.S. Supreme Court decision yet and limited appellate court decisions.[125] The basic legal analysis begins with the Fourth Amendment to the U.S. Constitution's protection against warrantless searches by law enforcement, absent special circumstances. Initially, the legal assumption was that a search meant a physical search of a location or a vehicle.[126] However, that area of the law has matured and developed. Fourth Amendment search and seizure jurisprudence includes the foundational Supreme Court cases: *Katz*,[127] *Kyllo*,[128] *Jones*,[129] *Jardines*,[130] *Riley*,[131] and most recently, *Carpenter*.[132] Each is discussed briefly below. Also discussed is the *Focia* case,[133] which has not reached the Supreme Court, and *Kahler*,[134] a lower court decision.

122. Steve Pote, *What Are Good Examples of (Legal) Uses of the Dark Web?*, QUORA (Feb. 21, 2016), https://www.quora.com/What-are-good-examples-of-legal-uses-of-the-Dark-Web [https://perma.cc/JJ2K-XNCR].

123. Steve Lohr, Mike Isaac & Nathaniel Popper, *Tech Hearings: Congress Unites to Take Aim at Amazon, Apple, Facebook and Google*, N.Y.TIMES (July 16, 2019), https://www.nytimes.com/2019/07/16/technology/big-tech-antitrust-hearing.html [https://perma.cc/RP9G-VEHT].

124. *See* Peter C. Ormerod, *A Private Enforcement Remedy for Information Misuse*, 60 B.C. L. REV. 1893 (2019), (https://ssrn.com/abstract=3340674 [https://perma.cc/2B4Y-ESZG]).

125. *Id.*

126. *See* Katz v. United States, 389 U.S. 347, 352 (1967).

127. *Id.*

128. Kyllo v. United States, 533 U.S. 27 (2001).

129. United States v. Jones, 565 U.S. 400 (2012).

130. Florida v. Jardines, 569 U.S. 1 (2013).

131. Riley v. California, 573 U.S. 373 (2014).

132. Carpenter v. United States, 138 S. Ct. 2206 (2018).

133. United States v. Focia, 869 F.3d 1269 (11th Cir. 2017)

134. United States v. Kahler, 236 F. Supp. 3d 1009 (E.D. Mich. 2017).

A. Katz v. United States

Cited as a seminal case in this area is *Katz v. United States*.[135] In *Katz*, the defendant objected to the use of evidence obtained by a warrantless wiretap on a phone booth he was using to conduct an illegal gambling business.[136] Katz lost at the district court and appellate court levels, but prevailed in the U.S. Supreme Court.[137] The Court introduced the analysis as follows:

> What a person knowingly exposes to the public, even in his own home or office, is not a subject of Fourth Amendment protection. *See Lewis v. United States,* 385 U. S. 206, 385 U. S. 210; *United States v. Lee,* 274 U. S. 559, 274 U. S. 563. But what he seeks to preserve as private, even in an area accessible to the public, may be constitutionally protected.[138]

B. Kyllo v. United States

In a case that may seem quaint due to the recent liberalization of marijuana laws in numerous states, *Kyllo vs. U.S.* deals with a situation in which law enforcement suspected that Kyllo was growing marijuana in his home.[139] Law enforcement officials used an infrared device from a nearby street to scan for hot spots in his home.[140] The device detects heat leakage from a building and the image on the screen of the hand-held device basically shows a type of halo around a building that emits excessive heat.[141] The suspected cause of such heat leakage in times when heat is not being used in most homes is that the resident is using extensive heat lamps to grow marijuana in the house.[142] Finding walls of his home to be unusually hot, they obtained a search warrant.[143] Indeed, they did discover high intensity lamps aiding the growth of marijuana plants.[144] The district court convicted Kyllo and the Ninth Circuit Court of appeals upheld the conviction.[145] Kyllo appealed to the US Supreme Court.[146] The key issue was whether Kyllo had a "subjective expectation of privacy" in his home such

135. *Katz*, 389 U.S. at 352**.** For an expanded discussion of the legal path to protection of Internet communications, see Sophia Dastagir Vogt, *The Digital Underworld: Combating Crime on the Dark Web in the Modern Era*, 15 SANTA CLARA J. INT'L L. 104, 111 (2017).
136. *Katz*, 389 U.S. at 350, 354.
137. *Id.* at 348, 359.
138. *Id.* at 351.
139. *Kyllo*, 533 U.S. at 29.
140. *Id.*
141. *Id.* at 29-30.
142. *Id.* at 30.
143. *Id.*
144. *Id.*
145. *Id.* at 30-31.
146. *See id.* at 31.

that an external search like the infrared scanner was a violation of his Fourth Amendment rights.[147] The Court held that Kyllo did have an expectation of privacy and that the use of the advanced infrared technology was beyond a simple observation by the naked eye, raising the technique to a search subject to the Fourth Amendment's protection.[148]

C. United States v. Jones

In *United States v. Jones*, Washington, D.C. nightclub owner Antoine Jones was suspected of cocaine trafficking.[149] Officials obtained a warrant that authorized the installation of a global positioning system (GPS) device on Jones' vehicle, to be installed in the District of Columbia within 10 days.[150] Despite this provision, the GPS installation did not take place until the eleventh day in Maryland, rendering the warrant invalid.[151] The GPS tracker produced more than 2,000 pages of information related to the activities of the target individual over the next twenty-eight days.[152] The Supreme Court ruled that the placement and tracking of the GPS device was an unauthorized, warrantless search of the subject's vehicle.[153] Justice Alito stated in his concurring opinion, "I conclude that the lengthy monitoring that occurred in this case constituted a search under the Fourth Amendment."[154]

D. Florida v. Jardines

In *Florida v. Jardines*, the Supreme Court, in an opinion written by Justice Scalia, considered, "whether using a drug-sniffing dog on a homeowner's porch to investigate the contents of a home is a 'search' within the meaning of the Fourth Amendment."[155] Without a warrant, detectives Pedraja and Bartelt approached the homeowner's front door with their drug detection dog who promptly signaled the strongest presence of drug odor coming from underneath the front door.[156] The Court held, "The government's use of trained police dogs to investigate the home and its immediate surroundings is a 'search' within the meaning of the Fourth Amendment."[157]

147. *Id.*
148. *See id.* at 40.
149. *Jones*, 565 U.S. at 402.
150. *Id.* at 402-03.
151. *Id.* at 403-04.
152. *Id.* at 403.
153. *Id.* at 413 (Alito, J., concurring).
154. *Id.* at 431.
155. *Florida v. Jardines*, 569 U.S. at 3.
156. *Id.* at 3-4.
157. *Id.* at 11-12.

E. Riley v. California

In *Riley v. California*, the police arrested David Riley for possession of concealed and loaded firearms discovered after stopping Riley for a traffic violation.[158] Incident to his arrest, a search of Riley produced a smartphone.[159] One of the arresting officers accessed information on the phone and noticed a term associated with the "Bloods" street gang.[160] The Court noted that Riley's phone had "a broad range of other functions based on advanced computing capability, large storage capacity, and Internet connectivity."[161] A detective specializing in street gangs later examined the contents of Riley's smartphone and observed "photographs of Riley standing in front of a car they suspected had been involved in a shooting a few weeks earlier."[162] As a result, Riley was eventually charged and convicted on three crimes connected to that earlier shooting.[163] Before his trial, Riley argued "that the searches of his phone violated the Fourth Amendment, because they had been performed without a warrant and were not otherwise justified by exigent circumstances."[164] On appeal, the Supreme Court ruled that due to the storage capacity of the modern smartphone, police must obtain a warrant before searching the suspect's phone.[165] Therefore, the search of Riley's smartphone was unconstitutional.[166]

F. Carpenter v. United States

On June 22, 2018, the U.S. Supreme Court announced its decision in *Carpenter v. United States*.[167] The Roberts court considered whether the government needs a search warrant to obtain voluminous records of a mobile phone's locational metadata, which is known as "cell site location information (CSLI)."[168] In *Carpenter*, four men were arrested during 2011 as suspects in a series of Radio Shack robberies.[169] Chief Justice Roberts wrote, "[o]ne of the men confessed that, over the previous four months, the group (along with a rotating cast of getaway drivers and lookouts)

158. *Riley v. California*, 573 U.S. at 378.
159. *Id.* at 378-79.
160. *Id.* at 378.
161. *Id.* at 379.
162. *Id.*
163. *Id.* at 379-80.
164. *Id.* at 379.
165. *Id.* at 403.
166. *Id.*
167. Carpenter v. United States, 138 S. Ct. 2206 (2018).
168. *See id.* at 2211.
169. *Id.* at 2212.

had robbed nine different stores in Michigan and Ohio."[170] Chief Justice Roberts concluded in the Court's opinion:

> The question we confront today is how to apply the Fourth Amendment to a new phenomenon: the ability to chronicle a person's past movements through the record of his cell phone signals. Such tracking partakes of many of the qualities of the GPS monitoring we considered in *Jones*. Much like GPS tracking of a vehicle, cell phone location information is detailed, encyclopedic, and effortlessly compiled.[171]

The decision emphasized the large amount of data that was obtained by "[m]apping a cell phone's location over the course of 127 days."[172] The Court noted that with GPS the detailed location information provided, "an intimate window into a person's life, revealing not only his particular movements, but through them his 'familial, political, professional, religious, and sexual associations.' These location records 'hold for many Americans the privacies of life.'"[173]

Extrapolating the Fourth Amendment analyses above to the search for the unique IP addresses and locations of the participants in Playpen, Silk Road, and other suspect websites, the question becomes whether law enforcement's use of the NIT and other hacking devices requires obtaining a search warrant before accessing the IP addresses of those participants. And, the analysis is more complicated because unlike in *Katz* and *Kyllo*, future suspects, subject to such hacking devices, may be in multiple states or even other countries.

G. United States v. Michael Albert Focia

The leading case regarding purchases on The Dark Web is the *United States v. Focia* in the U.S. Court of Appeals for the Eleventh Circuit.[174] Focia was convicted of dealing in firearms without a federal firearms license and selling firearms to persons in other states who did not possess firearms licenses.[175] Focia was convicted based on evidence gathered in a mechanical manner where federal agents simply purchased firearms from him and had them sent to other states.[176] The NIT was not used to locate him or his

170. *Id.*
171. *Id.* at 2216.
172. *Id.* at 2217.
173. *Id.*; *See also* Peter C. Ormerod & Lawrence J. Trautman, *A Descriptive Analysis of the Fourth Amendment and the Third-Party Doctrine in the Digital Age!,* 28 ALBANY L.J. SCI. & TECH. 73 (2018).
174. United States v. Focia, 869 F.3d 1269 (11th Cir. 2017).
175. *Id.* at 1274.
176. *Id.* at 1274-76.

computer.[177] The use of The Dark Web in Focia's case was primarily a vehicle to reach customers who could not purchase firearms legally.[178] His challenge to his conviction ranged from Second Amendment arguments to procedural arguments but did not directly raise the privacy issues related to The Dark Web.[179]

H. United States v. Kahler

There are a variety of U.S. District Court cases dealing with search warrants and The Dark Web. In *United States v. Kahler*, a 2017 Michigan case involving the Playpen site used by pedophiles, Kahler attempted to suppress the evidence against him that had been gathered through an FBI NIT.[180] The FBI received a lead that the Playpen server was located in the United States.[181] Following further investigation, the server was located in North Carolina and the owner was located in Florida.[182] The FBI moved the server to Virginia to then operate the site briefly in order to track users of the site.[183] However, the Tor software prevented the tracking of users.[184] The FBI then obtained the initial search warrant which was issued by a U.S. District Court Judge in Virginia and used the NIT to track users.[185] The FBI was able to track multiple pedophile customers, including Kahler.[186] The FBI then obtained a search warrant in the Michigan district where Kahler was located using the evidence gathered from the first search warrant.[187] Kahler moved to suppress the initial search warrant, which would defeat the basis for the Michigan warrant.[188]

The District Court's analysis of Kahler's Fourth Amendment challenge under Federal Rule of Criminal Procedure 41(b) to the search warrant included a review of the prior district court cases in this area.[189] The decision summarized the three most likely outcomes of such a challenge. First, the decision referenced twenty-two district court decisions holding that the NIT warrant was not properly issued, but denied the request to suppress the product of the search.[190] Second, the decision referenced eleven district court

177. *See id.*
178. *See id.* at 1274.
179. *See id.* at 1277-88.
180. United States v. Kahler, 236 F. Supp. 3d 1009 (E.D. Mich. 2017).
181. *Id.* at 1015.
182. *Id.*
183. *Id.*
184. *Id.*
185. *Id.*
186. *Id.*
187. *Id.*
188. *Id.*
189. *See id.* at 1017-18.
190. *Id.* at 1017 n.5.

decisions upholding the NIT warrant.[191] Third, as of the date of the decision, only four district courts had ruled to suppress the evidence obtained by the warrant.[192] Of these thirty-seven prior district court decisions, the location of the rulings appears fairly random as there is no obvious geographic preference for one of the three outcomes around the United States.[193]

The Kahler court essentially sided with the majority of district court decisions, concluding:

> [T]he FBI's solution to the technological issues posed by the Tor software was reasonable. Because of the FBI's good faith attempt to comply with existing law, despite its incompatibilities with the investigative realities faced, the fruits of the NIT warrant will not be suppressed.[194]

As referenced above, petitioner in the *Ulbricht* case petitioned the Supreme Court for certiorari in an attempt to avoid prosecution for activities on The Dark Web.[195] As in the cases discussed above, the main challenge to such prosecution is the legality of the search that led to the criminal prosecution. However, in the *Ulbricht* case, there was no warrant obtained by law enforcement.[196] The key argument by the prosecution is that the IP address obtained was not confidential information and therefore did not require a warrant.[197] Ulbricht's petition for certiorari also argued that his life sentence was too harsh under the Sixth Amendment,[198] but that argument is beyond the scope of this article. Ulbricht's case differs from the cases discussed immediately above because the NIT or other types of hacking procedures were not required to obtain the additional information that led to his prosecution; a job post in an online forum included Ulbricht's email address which authorities used to discover his IP address.[199] Given the Supreme Court's tradition of narrow rulings,[200] a decision in favor of Ulbricht or the prosecution would have been unlikely to resolve the issues raised by the NIT approach.

191. *Id.* at 1017 n.6.
192. *Id.* at 1018 n.7.
193. *Id.* at 1017 nn.5-7.
194. *Id.* at 1023.
195. *See generally* Blake, *supra* note 54.
196. *Id.*
197. *Id.*
198. *Id.*
199. Tim Hume, *How FBI Caught Ross Ulbricht, Alleged Creator of Criminal Marketplace Silk Road*, CNN (Oct. 5, 2013), https://www.cnn.com/2013/10/04/world/americas/silk-road-ross-ulbricht/index.html [https://perma.cc/U9WF-F2FL].
200. *See generally* Robert W. Scheef, *Temporal Dynamics in Statutory Interpretation: Courts, Congress and the Cannon of Constitutional Avoidance*, 64 U. PITT. L. REV. 529 (2003).

The *Stanford Law Review* article by Ahmed Ghappour, cited above, raises the issue of interference with international rights if the prosecutors in the United States use techniques such as the NIT to track users into other countries.[201] However, a commentary on this article in the next edition of the same publication challenges the very assumptions put forward by Ghappour.[202] In fact, the authors suggest that given the international interest by law enforcement in apprehending parties dealing in illegal weapons, drugs, pedophilia, identity theft and terrorism, other law enforcement agencies would welcome the potential assistance.[203]

Modern business practice is done by computer and most of those computers are linked to the Internet. Further, with the advancements in technology, virtually all portable computers, including laptops, notebooks, and now smart pads, like the iPad, access the internet as well. Smart phones also now have access to the internet. While traditional desktop computers are provided by employers, some employers today also provide portable computers and smart phones to their employees.[204] The obvious reason for this is to increase the productivity of employees and enable them to communicate more effectively with their workplaces as well as with customers and vendors. Without direct connection to the internet, most of these devices would contribute far less to employee productivity.

The risks to employers are obvious and growing.[205] An employee utilizing his or her workplace computer or wireless device to access The Dark Web is exposing the employer's device, not a personal device. With the use of the NIT and similar hacking techniques, the location and identification of the device will be to the employer's, not the employee's, location. While in response to an investigation, the employer could identify the employee who had access to the specific device; the starting point will still be the employer's hardware. Further, press reports and court records will reflect the path of the evidence, and that will include the employer's identification. The potential harm to an employer's business by

201. Ghappour, *supra* note 14, at 1108-22.

202. Orin S. Kerr & Sean D. Murphy, *Government Hacking to Light the Dark Web: What Risks to International Relations and International Law?,* 70 STAN. L. REV. ONLINE 58 (2017).

203. *Id.* at 62-65.

204. *Cf.* Eric McCarthy, *New Study Shows Critical Role of Smartphones in Workforce Productivity,* SAMSUNG INSIGHTS (June 26, 2017), https://insights.samsung.com/2017/06/26/new-study-shows-growing-role-of-cellphones-at-work [https://perma.cc/NUU3-4QZ9] (article questions why "more companies [aren't] providing phones to their employees, like they do desktops or other key equipment?").

205. Lisa McGlynn, *What Employers Need to Know About the Dark Web*, SHRM (May 8, 2018), https://www.shrm.org/ResourcesAndTools/hr-topics/technology/Pages/Employers-Need-to-Know-About-Dark-Web.aspx [https://perma.cc/ASU5-VMNR].

being reported as a portal used to view pedophilia or purchase illegal drugs could be substantial, even if there is no attempt to involve the employer in the prosecution of the employee involved.

III. RECOMMENDATIONS FOR EMPLOYERS

It is the responsibility of every organization in the current risky cyber environment to take all reasonable steps to ensure that the computer systems and related devices used by the modern organization are as safe as possible. This applies equally to the public and private sectors of the economy.[206] Not only do managers and officers have such responsibility, the board of directors, in performing governance responsibilities, should review the steps that have been taken to ensure the integrity of its data systems from cyberattack.[207] Rapid technological change results in ongoing challenges to the management of cyber risk.[208]

The U.S. Department of the Treasury prepared a list of ten questions any enterprise can use to think about cybersecurity.[209] These questions, while drafted to meet the particular needs of banks, can be tailored to fit the needs of any line of business. Deputy Treasury Secretary Sarah Bloom Raskin explained that, "at Treasury we have framed our thinking about cybersecurity and financial industry preparedness against cyber-attacks around three categories of activities: (1) baseline protections, (2) information sharing, and (3) response and recovery."[210] Blocking employee access to The Dark Web would fall under baseline protections and

206. *See generally* Lawrence J. Trautman, *Congressional Cybersecurity Oversight: Who's Who & How It Works,* 5 J.L. & CYBER WARFARE 147 (2016); Lawrence J. Trautman, *Cybersecurity: What About U.S. Policy?,* 2015 U. ILL. J.L. TECH. & POL'Y 341 (2015).

207. *See generally* Lawrence J. Trautman & Janet Ford, *Nonprofit Governance: The Basics*, 52 AKRON L. REV. 971 (2018); Lawrence J. Trautman, *Managing Cyberthreat,* 33 SANTA CLARA HIGH TECH. L.J. 230 (2017); Lawrence J. Trautman & Kara Altenbaumer-Price, *The Board's Responsibility for Information Technology Governance*, 28 J. MARSHALL J. COMPUTER & INFO. L., 313 (2011); Lawrence J. Trautman, *Governance of the Facebook Privacy Crisis*, 20 PITT. J. TECH L. & POL'Y (2020) http://ssrn.com/abstract=3363002 [https://perma.cc/E64Y-X4ZS]; Lawrence J. Trautman, *The Matrix: The Board's Responsibility for Director Selection and Recruitment,* 11 FLA. ST. U. BUS. REV. 75 (2012).

208. *See generally* Lawrence J. Trautman & Mason J. Molesky, *A Primer for Blockchain*, 88 UMKC L. REV. (2019); Lawrence J. Trautman, *How Google Perceives Customer Privacy, Cyber, E-commerce, Political and Regulatory Compliance Risks*, 10 WM. & MARY BUS. L. REV. 1 (2018); Lawrence J. Trautman, *E-Commerce, Cyber, and Electronic Payment System Risks: Lessons from PayPal,* 16 U.C. DAVIS BUS. L.J. 261 (2016); Lawrence J. Trautman, *Is Disruptive Blockchain Technology the Future of Financial Services?,* 69 THE CONSUMER FIN. L.Q. REP. 232 (2016).

209. Remarks of Deputy Secretary Raskin at The Texas Bankers' Association Executive Leadership Cybersecurity Conference: Cybersecurity for Banks: 10 Questions for Executives and Their Boards, U.S. DEP'T TREASURY (Dec. 3, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl9711.aspx [https://perma.cc/Z6QT-3W5J].

210. *Id.*

hopefully, avoid some of the need for response and recovery following a cyber attack.

As noted in the Overview and Part II, The Dark Web has a history of being used for nefarious purposes, including illegal drugs, illegal sale of weapons, pedophilia, sale of identities, ransomware, and tools for terrorism. Some might argue that there are at least two legitimate purposes for an employee to utilize The Dark Web. First, to protect their identity while they act as a whistleblower against either their employer or another entity; or, second, reporters could use this anonymity to protect sources for sensitive articles involving corruption or crimes. In fact, even the *Kahler* court includes this language regarding the use of The Dark Web: "Given the rise of 'targeted' online advertisements which use observed information about the user's online habits to individually tailor advertisements, a desire for online anonymity is neither unreasonable nor suspicious."[211]

Employers could monitor employee activity while on the web to try to detect access to or downloading of improper materials from the Internet while at work or on work time away from work.[212] However, such monitoring brings its own problems. Some states restrict monitoring employees while they are at work.[213] Further, some federal agencies have raised concerns regarding whether monitoring might be used to limit employee attempts to unionize, or employee exchanges of information regarding salary and issues related to discrimination.[214] Another possible concern is that if employers indicate that they will monitor employees and then an employer could have detected the downloading of illegal materials, but did not do so, law enforcement may imply that the employer knew of such conduct, but was complicit since the employer did not refer such actions to law enforcement.

211. *United States v. Kahler*, 236 F. Supp. 3d at 1021.

212. *See USA Employee Monitoring Laws: What Are Employers Allowed and Not Allowed Doing in the Workplace?*, WORKTIME (Aug. 19, 2016), https://www.worktime.com/usa-employee-monitoring-laws-what-can-and-cant-employers-do-in-the-workplace [https://perma.cc/GKF5-W3BD]. *See also* Martha Zackin, *No Expectation of Privacy in Emails Sent Over Employer's Email Account, Massachusetts Court Decides*, MINTZ (May 21, 2012), https://www.employmentmattersblog.com/2012/05/no-expectation-of-privacy-in-emails-sent-over-employers-email-account-massachusetts-court-decides [https://perma.cc/8G3Z-J8CA].

213. *See Workplace Privacy and Employee Monitoring*, PRIVACY RIGHTS CLEARINGHOUSE (Mar. 1, 1993), https://www.privacyrights.org/consumer-guides/workplace-privacy-and-employee-monitoring [https://perma.cc/ZVG6-TX2T]; *see also* Brenda R. Sharton & Karen L. Newman, *The Legal Risks of Monitoring Employees Online*, HARV. BUS. REVIEW (Dec. 14, 2017), https://hbr.org/2017/12/the-legal-risks-of-monitoring-employees-online [https://perma.cc/XZ3T-JGYN].

214. *See Prohibited Employment Policies/Practices*, U.S. EQUAL EMP'T OPPORTUNITY COMM'N, https://www.eeoc.gov/laws/practices/index.cfm [https://perma.cc/6L5C-7X8Z].

In addition to the legal risks of monitoring employees, the cost of monitoring needs to be considered. While technology makes it possible to monitor what employees do on their office computers, expanding that monitoring to the wider range of devices which now includes laptops, notebooks, iPads and smart phones makes this a larger and more costly proposition.

A more complete and less risky proposition would be for employers to block all access to sites that are not indexed on the WWW on employer-provided computers and other devices. Technology exists today to do this for organizations large and small, either with hardware or software.[215] Further, while many employers already include in employee handbooks and employee training the need for employees to work while on work time, employers should continue to emphasize that "surfing the web" or other activities that are not work related are prohibited. In particular, any dealing in Bitcoins and other virtual currency is very unlikely to be a work-related activity and as noted, this is the coin of the realm in the underworld of The Dark Web.[216]

As discussed above, there are some limited legitimate uses of The Dark Web. However, the few employees who have a legitimate need for privacy have access to alternative websites on their own equipment and should not find the unavailability of The Dark Web on their employer-provided devices a significant obstacle.

CONCLUSION

As the Internet approaches its 30th Anniversary, the "web" is still growing and changing. The use of the Internet for all types of business purposes makes it an indispensable tool. However, employers must be continually alert to the risks posed by the same tool that provides so much that is positive. Employers have continued to upgrade their SPAM filters, moved to educate employees about avoiding viruses and phishing emails, and the dreaded ransomware attacks. Adding The Dark Web to these concerns is best avoided by employers by blocking access entirely.

215. Adam Rice, *Tor Networks: Stop Employees from Touring the Deep Web*, TECHTARGET (Feb. 3, 2014), https://searchsecurity.techtarget.com/feature/Tor-networks-Stop-employees-from-touring-the-deep-Web [https://perma.cc/KXS5-SHTP].

216. *Id.*