Journal of International Business and Law

Volume 21 | Issue 2 Article 6

3-1-2022

The Complexities of International Cybercrime and Security: Updating Laws for a New Digital Age

Jesslyn Bracco

Follow this and additional works at: https://scholarlycommons.law.hofstra.edu/jibl

 Part of the Law Commons

Recommended Citation

Bracco, Jesslyn (2022) "The Complexities of International Cybercrime and Security: Updating Laws for a New Digital Age," *Journal of International Business and Law*: Vol. 21: Iss. 2, Article 6.
Available at: https://scholarlycommons.law.hofstra.edu/jibl/vol21/iss2/6

This Note is brought to you for free and open access by Scholarship @ Hofstra Law. It has been accepted for inclusion in Journal of International Business and Law by an authorized editor of Scholarship @ Hofstra Law. For more information, please contact lawscholarlycommons@hofstra.edu.

THE COMPLEXITIES OF INTERNATIONAL CYBERCRIME AND SECURITY: UPDATING LAWS FOR A NEW DIGITAL AGE

Jesslyn Bracco

I. INTRODUCTION

A. The Evolution of Technology

1. The Increased Use of Electronic Storage Databases

Changes in technology have allowed us to generate and store large amounts of data.[1] An early method of mechanized storage dates back to the nineteenth century in the form of punch cards.[2] Then, in 1932, Gustave Tausche developed the Magnetic Drum, which was a "long metal cylinder coated in magnetic recording material, with rows of read-write heads on the axis of the drum."[3] Next, the Williams-Kilburn Tube was created, this included the use of a cathode ray tube to store dots on the screen's surface, and was the primary form of storage in 1947.[4] In 1951, the Magnetic Tape Drive utilized a plastic film with a magnetic coating for data recording.[5] Common examples of this included cassette tapes and Video Home System ("VHS") tapes.[6] In 1956, the Hard Disk Drive was created.[7] When it was first introduced, VHS tapes weighed over a ton; now they fit in the palm of an adult hand.[8] Subsequent storage systems include the floppy disk, compact disc, zip drive, digital video disc, SD card, USB flash drives, and Blu-ray optical disc.[9] Starting in 2006, cloud data storage became the most popular form of data storage.[10] Remote databases became accessible with internet access and, depending on the plan, can store seemingly endless amounts of data.[11] "Experts estimate more than 2,700,000,000,000,000,000KB of data exists in the digital universe today."[12]

---

[1] *Timeline of Computer History*, COMPUTER HISTORY MUSEUM, https://www.computerhistory.org/timeline/memory-storage/ (last visited Sept. 10, 2021).

[2] *The History of Computer Data Storage, in Pictures*, SOLARWINDS PINGDOM (Apr. 12, 2019), https://www.pingdom.com/blog/the-history-of-computer-data-storage-in-pictures/.

[3] *Magnetic Drums*, COMPUTER HISTORY MUSEUM, https://www.computerhistory.org/revolution/memory-storage/8/252 (last visited Mar. 22, 2022).

[4] *Timeline of Computer History*, *supra* note 1.

[5] Mollee Shannon, *History of the VHS Tape*, KODAK, https://kodakdigitizing.com/blogs/news/history-of-the-vhs-tape (last visited Mar. 22, 2022).

[6] *Id.*

[7] *Timeline of Computer History*, *supra* note 1.

[8] *Id.*

[9] *Id.*

[10] *Id.*

[11] *Id.*

[12] *See Data Storage Devices Timeline,* FRONTIER, https://www.frontierinternet.com/gateway/data-storage-timeline/ (last visited Sept. 10, 2021).

Published by Scholarship @ Hofstra Law, 2022

2. The Basis for Cyber Attacks

Businesses of all sizes can be the targets of cyber-attacks, since they collect sensitive information that criminals may seek to exploit.[13] Cybercriminals typically carry out attacks in search of "a business's financial details, customer's credit card data, sensitive personal data, customer's or staff's credentials, customer databases, clients lists, IT infrastructure, IT services, and intellectual property."[14] Financial gain motivates most cybercriminals, which they obtain either by holding the information for ransom or from selling the information they steal to others on the dark web.[15]

Some cyber-attacks are carried out to make a social or political point, others to spy on competitors or other organizations, and still, others to engage in so-called "ethical hacking" for sport or an intellectual challenge.[16] A group that engages in cyber hacking for the purpose of making social or political statements, for example, is the re-emerged organization called Anonymous.[17] Anonymous gained recent media attention when they carried out various cyber-attacks during the George Floyd protests in the United States in order to make a statement against the government and police.[18]

II. BACKGROUND/HISTORY

A. Types of Hacking

Malware attacks can occur when a party installs malicious software onto the user's computer without consent.[19] The malicious software comes in various forms of viruses, spyware, or ransomware. This malicious software accesses private networks, interrupts communication on a network, steals sensitive information, and sometimes inspects the user's activity over a long period.[20] The most common types of malware are viruses, worms, trojans, ransomware, and spyware.[21] Once worms access the target device, their goal is to spread across the network or system of networks to infect other devices to gain information.[22] Trojans hide in programs to create what are called "backdoors," which provide undetectable access for the hackers to collect the information on the computer.[23] Ransomware locks the information and then demands payment for the same information to be released to its user or

[13] *See Cyber Security for Business*, NI BUSINESS INFO, https://www.nibusinessinfo.co.uk/content/reasons-behind-cyber-attacks (last visited Sept. 10, 2021).

[14] *Id.*

[15] *See id.*

[16] *Id.*

[17] *See* David Molloy & Joe Tidy, *George Floyd: Anonymous hackers re-emerge amid US unrest*, BBC, https://www.bbc.com/news/technology-52879000 (last visited Sept. 10, 2021).

[18] *See id.*

[19] *See* Jibi Mariam Biju et al., *Cyber Attacks and Its Different Types,* 06, INT'L RESEARCH J. OF ENG'G AND TECH., 4849, 4851 (2019) (describing malware attacks).

[20] *See id.*

[21] *Id.*

[22] *See id.*

[23] *Id.*

owner.[24] Finally, Spyware is malware that inspects the user's activity and reports it to the hacker.[25]

One of the most common types of attacks is phishing attacks.[26] The primary goal of this attack is to gain personal and credential information.[27] These types of attacks include hyperlinks.[28] By clicking on the hyperlink, the party installs malicious software onto the computer or device.[29] Alternatively, a hyperlink will bring the user to another browser and will ask for personal information, which, if provided, is sent to the hacker.[30] Phishing attacks can take the form of messages, calls, emails, and fake websites.[31]

Denial-of-Service ("DoS") and distributed denial-of-service attacks ("DDoS") overload the system so that it cannot complete a service or repair.[32] This method of attack differs from a phishing attack; instead of clicking a hyperlink, the hacker floods a network server with traffic.[33] Instead of targeting individual devices, DoS targets a server or a network.[34] The hackers send so many requests that the server cannot process the junk requests fast enough, it can no longer respond or it crashes.[35] The malware makes the computer's resources unavailable by disrupting the service of the host that is connected to the internet.[36] This type of attack is difficult to prevent.[37]

Advanced Persistent Threats ("APTs") are attacks that target different vulnerabilities in the network to create or establish backdoors within the service infrastructure to withdraw information over a long period without being discovered.[38] Most of the time businesses are unaware that they are under attack, which allows the hacker to access sensitive data, and to place other various forms of malware into the system.[39] Unlike some forms of hacking such as Denial-of-Service, APTs are created to attack a specific or targeted company or organization and are highly sophisticated in design.[40]

The United States Federal Trade Commission ("FTC") created an online reporting form in which a victim may fill out if they suspect malware has been downloaded onto their

---

[24] *Id.*

[25] *See id.*

[26] *See id.* at 450.

[27] *See id.*

[28] *Id.*

[29] *See id.*

[30] *See id.*

[31] *Id.* at 4851.

[32] *Id.* at 4849.

[33] *Understanding Denial-of-Service Attacks*, DEP'T OF HOMELAND SEC., (Nov. 4, 2009), https://us-cert.cisa.gov/ncas/tips/ST04-015.

[34] *See id.*

[35] *See id.*

[36] Biju et al., *supra* note 19, at 4849.

[37] *Id.*

[38] *Advanced Persistent Threat (APT)*, NAT'L INST. OF STANDARDS AND TECH., https://csrc.nist.gov/glossary/term/advanced_persistent_threat (last visited Sept. 10, 2021).

[39] *See* Nate Lord, *What is an Advanced Persistent Threat? APT Definition*, DATAINSIDER (Sept. 11, 2018), https://digitalguardian.com/blog/what-advanced-persistent-threat-apt-definition.

[40] *Id.*; *See* Molloy & Tidy, *supra* note 17.

device or network.[41] The online form inquires about what happened so the information can be further used to investigate the cyber-attack.[42] The FTC provides information for how a person would protect themselves and explains how the FTC shares information with law enforcement.[43] Lists created by the FTC include possible indicators that may connote a malware attack.[44] Some of the indicators include the "device suddenly crashing, slowing down, refusing to shut down or restart, running out of battery life quickly, showing unsuspecting toolbars or icons, and showing ads in unusual places."[45] The FTC provides further advice for users instructing how to remove malware, how to avoid downloading malware, and how to get help from a third-party.[46]

B. Sanctioning the Conduct Through Legislation: The CFAA and NYCRR part 500

1. Federal Law

The Comprehensive Crime Control Act of 1984 included the first federal computer fraud statute.[47] The law was later codified as 18 U.S.C. § 1030.[48] It prohibited "fraud and related activity in connection with computers," meaning the "knowing access without authorization" to do so or "exceeding access."[49] The law was later amended in 1986 and is referred to as the Computer Fraud and Abuse Act ("CFAA").[50] The CFAA is the primary mechanism in the United States for prosecuting cybercrime and providing civil and criminal penalties.[51] The CFAA expanded the protection provided under the computer fraud statute.[52] The CFAA "prohibits unauthorized access or exceeding authorization to a computer, knowingly accessing a protected computer without authorization, trafficking passwords, and transmitting threats and/or demands of extortion for money or property."[53] Congress increased

---

[41] *Report to Help Fight Fraud*, FED. TRADE COMM'N, https://reportfraud.ftc.gov/#/?pid=B (last visited Nov. 10, 2021).

[42] *Id.*

[43] *See generally id.* (The FTC website provides the individual with resources such as, how to get money back when the individual has sent the hacker money, what to do if the individual thinks their device has been affected by malware, and what an individual needs to do to file a report).

[44] *Consumer Information*, FED. TRADE COMM'N, https://www.consumer.ftc.gov/articles/how-recognize-remove-and-avoid-malware (last visited Nov. 10, 2021).

[45] *Id.*

[46] *See id.* The FTC provides ways for an individual who believes they have been hacked to remove the malware themselves and the steps necessary to do so, the FTC suggests that the individual contact the manufacturer of the device for tech support, and where to report malware both on the FTC website and the FBI complaint center.

[47] Comprehensive Crime Control Act, Pub. L. No. 98-437, 98 Stat. 1976; 18 U.S.C. § 1030 (1986). *See CFAA Background*, NAT'L ASSOC. OF CRIM. DEF. LAW. (March 10, 2020), https://www.nacdl.org/Content/CFAA Background.

[48] *Id.*

[49] 18 U.S.C. § 1030; Comprehensive Crime Control Act, Pub. L. No. 98-437, 98 Stat. 1976.

[50] *See* Computer Fraud and Abuse Act, Pub. L. No. 99-474, 100 Stat. 1213; *Computer Fraud and Abuse Act* [hereinafter "CFAA"], NAT'L ASSOC. OF CRIM. DEF. LAW., https://www.nacdl.org/Landing/Computer FraudandAbuseAct (last visited Sept. 10, 2021); NAT'L ASSOC. OF CRIM. DEF. LAW., *supra* note 47.

[51] 18 U.S.C. § 1030; *see also Computer Fraud and Abuse Act*, *supra* note 50.

[52] NAT'L ASSOC. OF CRIM. DEF. LAW., *supra* note 47.

[53] 18 U.S.C. § 1030(a)(1) (1986).

the protection by expanding the scope of indictable conduct to include the transmission of threats or extortion and outlaws altering, damaging or destroying information.[54] Punishments under the CFAA include fines or imprisonment depending on the severity of violation.[55] However, in 1994, the CFAA was amended to include a civil cause of action, which provided victims with a remedy to for compensatory damages, injunctive relief, and other equable forms or relief.[56]

The CFAA neglected to define what "without authorization" or "in excess of authorization" meant.[57] In a decision rendered on June 3, 2021, the United States Supreme Court provided guidance on what constitutes "exceed[ing] authorized access."[58] The Supreme Court narrowly tailored the definition to mean to "access a computer with authorization but then obtains information located in particular areas of the computer – such as files, folders, or databases that are off limits" to him or her.[59] The definition narrows the scope of the statute to prohibit trespass on computers or networks, meaning punishing those not given permission to be on the computer or network and those that were given permission but went farther than permitted.[60]

2. New York Law

Starting March 17, 2017, the State of New York ("NY") began regulating cybersecurity by imposing requirements intended to protect information systems and private information stored within such systems.[61] The New York Codes, Rules and Regulations ("NYCRR") Part 500 applies to entities that operate under a license or registration under NY banking law, insurance law, or financial services law.[62] It requires all entities to protect the confidentiality of the information stored thereby requiring the assessment of internal and external risks, implement organization-wide policies and procedures to protect the information, monitoring for any suspicious activity, and recovering and restoring data after any event that affects the organization's operations.[63]

The New York Department of Financial Services ("DFS") promulgated these regulations to monitor threats to "information and financial systems by nation-states, terrorist organizations and independent criminal actors."[64] Part 500 requires all covered entities to "implement and maintain written policies, approved by a Senior Officer, or the covered

---

[54] NAT'L ASSOC. OF CRIM. DEF. LAW., *supra* note 47.

[55] 18 U.S.C. § 1030(c) (1986).

[56] NAT'L ASSOC. OF CRIM. DEF. LAW., *supra* note 47.

[57] 18 U.S.C. § 1030 (1986). *See also Computer Fraud and Abuse Act*, *supra* note 50.

[58] Van Buren v. United States, 141 S. Ct. 1648 (U.S. June 3, 2021).

[59] *Id.*

[60] *Id. See* Jonathan Mollod & Jeffrey Neuburger, *Supreme Court Ends Long-Running Circuit Split over CFAA "Exceeds Authorized Access" Issue, Adopting a Narrow Interpretation That Will Reverberate in Scraping Disputes and Litigation Over Departing Employees*, JDSUPRA (June 7, 2021), https://www.natlawreview.com/article/supreme-court-ends-long-running-circuit-split-over-cfaa-exceeds-authorized-access.

[61] Anjali C. Das, *New York Cracks Down on Cybersecurity Compliance*, THE NAT'L L. REV. (Aug. 9, 2021), https://www.natlawreview.com/article/new-york-cracks-down-cybersecurity-compliance.

[62] *See id*; 23 NYCRR § 500 (2017).

[63] 23 NYCRR § 500.02 (2017). *See* Das *supra* note 61.

[64] 23 NYCRR § 500.00 (2017).

entity's board of directors."[65] Such policies include implementing employee training;[66] conducting evaluations that identify potential risks or vulnerabilities in their systems;[67] multi-factor authentication;[68] and establishing an incident response plan to respond and recover from any event that affects the entity's information systems.[69] All entities must provide notice to DFS of any attempt or successful act to gain unauthorized access to disrupt or misuse the entity's information system or the information stored on such systems.[70] These rules impose a duty on companies to regulate and maintain their own security rather than placing the burden on government to step in and maintaining the data.[71]

III. LEGAL ISSUES

The nature of the internet requires the protection of private information to extend beyond state and national borders.[72] The first form of international law in this area is the Council of Europe Convention on Cybercrime, also referred to as the Budapest Convention, with sixty-six member states as parties to the convention.[73] Eleven more "have signed it or been invited to accede."[74] While this is the governing international law, the convention is materially flawed because it fails to address, or properly critical issues of substantive, procedural, and evidentiary law, such as cloud storage and the sharing of electronic evidence that will help with investigations for criminal and civil cases.[75] The Budapest Convention failed to expand or explain the substantive criminal law such as "illegal access, data interference, and system interference."[76] Thus, there are currently no consequences for individuals who commit international cybercrimes using these methods.[77]

The Second Additional Protocol to the Budapest Convention was added to criminalize racist or xenophobic acts committed through computer systems.[78] The United

---

[65] 23 NYCRR § 500.03 (2017).

[66] 23 NYCRR § 500.16 (2017).

[67] 23 NYCRR § 500.09 (2017).

[68] 23 NYCRR § 500.12 (2017).

[69] 23 NYCRR § 500.16 (2017).

[70] 23 NYCRR § 500.17 (2017); Das, *supra* note 61.

[71] *See* 23 NYCRR § 500.16 (2017).

[72] *See Data Protection Legislation*, UNITED NATIONS OFF. OF DRUGS AND CRIME, https://www.unodc.org/e4j/en/cybercrime/module-10/key-issues/data-protection-legislation.html (last visited Sept. 11, 2021).

[73] *See* Convention on Cybercrime, Nov. 23, 2001 – Mar. 17, 2017, E.T.S. No. 185, T.I.A.S. No. 13174. *See Budapest Convention and Related Standards*, COUNS. OF EUR. PORTAL, https://www.coe.int/en/web/cybercrime/the-budapest-convention-old (last visited Sept. 11, 2021).

[74] Convention on Cybercrime, Nov. 23, 2001 – Mar. 17, 2017, E.T.S. No. 185, T.I.A.S. No. 13174; *Parties/Observers to the Budapest Convention and Observer Organisation to the T-CY,* COUNCIL OF EUR., https://www.coe.int/en/web/cybercrime/parties-observers (last visited Oct. 23, 2021).

[75] *See* Jennifer Daskal & Debrae Kennedy-Mayo, *Budapest Convention: What is it and How is it Being Updated?*, CROSS BORDER DATA FORUM (July 2, 2020), https://www.crossborderdataforum.org/budapest-convention-what-is-it-and-how-is-it-being-updated/.

[76] Convention on Cybercrime, Nov. 23, 2001 – Mar. 17, 2017, E.T.S. No. 185, T.I.A.S. No. 13174.

[77] *See id.*

[78] Additional Protocol to the Convention on Cybercrime, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems, Jan. 28, 2003 – May 19, 2017, E.T.S. No. 189; *Sweden Joins the Budapest Convention and its Additional Protocol*, COUNS. OF EUR. (Apr. 28, 2021), https://www.coe.int/en/web/cybercrime/-/sweden-joins-the-budapest-convention-and-its-additional-protocol.

Nations ("UN") has tried to fill the gaps posed by the Budapest Convention by proposing the creation of a new cybercrime treaty; the committee in charge of drafting the treaty consists of experts from around the world.[79] When taken to a vote in December 2019, the UN General Assembly was divided on fundamental aspects of the treaty such as what constitutes cybercrime, how law enforcement gains access for evidence and data in cross-border investigations, and the role of government regulation on the internet.[80]

This Note will address the following four issues: (1) What are the current international laws currently govern cybercrime?;[81] (2) What is the proposed treaty attempting to accomplish?; (3) What obligations does the proposed treaty place on companies, organizations, and other legal persons?; (4) Finally, if widely accepted, what are the privacy concerns that the proposed treaty presents?

A. Current Laws Governing Cybercrime?

1. International Laws

At the international level, the Budapest Convention aims to create cybercrime laws for all signatory states.[82] Over sixty nation-states, including the United States and the United Kingdom, signed the Budapest Convention on November 23, 2001, and it became effective in 2004.[83] The Committee of Foreign Relation's Report clearly laid out that the purpose of the Budapest Convention was to "enhance the investigation and prosecution of cross-border computer-related crimes by eliminating procedural and jurisdictional obstacles to international cooperation."[84] The treaty established criminal offenses for "intentional illegal access to the whole or part of a computer system without consent and intentionally illegal interception of computer data to, from or within a computer system, data interference, system interference, misuse of devices, computer-related forgery, and computer-related fraud."[85] The Budapest Convention has been beneficial as it provides: a "legal basis for international cooperation on cybercrime and electronic evidence," ability to share information and experience, and access to a "network of practitioners."[86] "Misuse of device" is "the production, sale, procurement for use, import, distribution or otherwise making available of: a device — including a computer program, a computer password code or possession of the aforementioned items."[87] Computer-related forgery prohibits "intentionally without consent

---

[79] *See UN Approves Timetable for New Treaty to Combat Cybercrime*, ASSOCIATED PRESS (May 27, 2021), https://apnews.com/article/united-nations-general-assembly-united-nations-technology-06be1f9990a541ecdeb25ab01fc89df1.

[80] Deborah Brown, *Cybercrime is Dangerous, But a New UN Treaty Could be Worse for Rights*, HUMAN RIGHTS WATCH (Aug. 13, 2021), https://www.hrw.org/news/2021/08/13/cybercrime-dangerous-new-un-treaty-could-be-worse-rights#.

[81] Daskal & Kennedy-Mayo, *supra* note 75.

[82] *See* Convention on Cybercrime, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.

[83] *See id.*

[84] S. REP. NO. 109-6, at 1 (2005).

[85] Convention on Cybercrime, art. 2-8, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.

[86] COUNS. OF EUR., THE BUDAPEST CONVENTION ON CYBERCRIME: BENEFITS AND IMPACTS IN PRACTICE, 44 (2020).

[87] Convention on Cybercrime, art. 6, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.

inputs, alterations, deletion, or suppression of computer data, which results in inauthentic data with the intent that it is considered to be authentic."[88] Computer-related fraud prohibits "intentional, without consent, use that causes a loss of property to another by any input, alteration, deletion, or suppression of computer data or any interference with the functioning of a computer system with fraudulent or dishonest intent of procuring an economic benefit for oneself or another."[89] The Budapest Convention permits civil litigation that may result in monetary damages.[90]

The Budapest Convention has helped guide domestic legislation worldwide.[91] The Senate concluded that "No new implementing legislation is required to for the Convention. An existing body of federal laws will suffice to implement the obligations of the convention, although some minor reservations and declaration are needed..."[92] Many states have done just that, Spain created and implemented several amendments of substantive legislation pertaining to cybercrime and related procedural powers to meet the Budapest Convention's requirements.[93] Spain has noted that it uses the Budapest Convention as a resource beyond their own domestic legal guides and training materials.[94] Peru updated its cybercrime laws in 2013 and 2014 to include crimes against "data and information systems, including illegal access and attacks on the integrity of data systems, child exploitation offenses, illegal trafficking in data and interception of data, electronic fraud, and crimes relating to identity theft and abuse of devices"[95] In 2004, Romania implemented the Budapest Convention into its own legislation and further ratified the Additional Protocol that criminalizes racist and xenophobic computer acts.[96] There are sixteen countries that have used the Budapest Convention as a guideline for their own domestic legislation.[97]

Organizations such as the Human Rights Watch and the ACLU have spoken out to oppose the adoption of the Budapest Convention and any further international cybercrime treaties.[98] The ACLU has argued that the Budapest Convention lacked protections for privacy and civil liberties.[99] The treaty required that the signatory states to allow searches and seizures without a fee, which might encourage the police in various states to abuse their power.[100] Police may make any search and seizure without any economic constraints.[101] Progressive organizations like these argue that the treaty is too broad, that it provides police power to surveil using "internet-tapping" and similar devices, and object to the manner in which the

[88] Convention on Cybercrime, art. 7, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.

[89] Convention on Cybercrime, art. 8, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.

[90] *See* Convention on Cybercrime, arts. 12 & 13, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.

[91] *See* COUNS. OF EUR., *supra* note 86, at 6-7.

[92] S. REP. NO. 109-6, at 6 (2005).

[93] COUNS. OF EUR., *supra* note 86, at 7.

[94] *See id.*

[95] *Id.*

[96] *Id.*

[97] *See id.* at 6-7.

[98] *See* Brown, *supra* note 80. *See also* ACLU, *Seven Reasons the US Should Reject the International Cybercrime Treaty*, https://www.aclu.org/other/seven-reasons-us-should-reject-international-cybercrime-treaty (last visited Jan. 19, 2022).

[99] ACLU, *supra* note 98.

[100] *Id.*

[101] *See id.*

treaty was drafted because did not hold hearings or otherwise permit industry, public interests groups, and civil society to supply any import or voice their concerns.[102] While conceding that "cybercrime poses a real threat to people's human rights and livelihoods," Human Rights Watch insist that "efforts to address [cybercrime] need to protect, not undermine, rights."[103] The agreement between the US and the UK under the Clarifying Lawful Overseas Use of Data ("CLOUD") Act created concerns of government infringement upon individual's rights.[104] Under the terms of the treaty, one of the signatories may demand electronic data from service providers in the other country and authorizes US officials to access subscriber information from the UK providers.[105] The worry is that the release of information falls short of the Fourth Amendment of the U.S. Constitution and is not narrowed to specific circumstances where the information is necessary to prevent harm to life and safety.[106] Progressive Organizations have suggested that individual governments should bolster their own laws and resources to manage cybercrime rather than pursue international treaties.[107] While this suggestion seems self-explanatory, it fails to address how individual countries should cooperate to combat international cybercrimes.[108]

The Organization for Economic Co-operation and Development (OECD) is an intergovernmental organization that collaborates with governments, policymakers, and citizens and aims to improve economic performance and create jobs.[109] The OECD released privacy guidelines, which address "basic problems of protection of privacy and individual liberties" and sets forth principles to address the issues, as well as improve collaboration among states.[110] Such guidelines set forth that a person or entity that controls data should have a privacy management program that is "tailored to the structure, scale, volume and sensitivity" of the operations and implements the proper safeguards.[111] The guidelines further suggest that a member country should refrain from "restricting transborder flows of personal data between itself and another country" where either it follows the guidelines or sufficient safeguards exist.[112] The guidelines aim to facilitate "cross-border privacy law enforcement cooperation" to aid in effective investigative procedures.[113] The OCED states that by forming "[a] strong global network of privacy enforcement authorities working together is the first

---

[102] *Id.*

[103] Clarifying Lawful Overseas Use of Data Act, Pub. L. 115-141, 132 Stat. 1213; *Groups Urge Congress to Oppose US-UK Cloud Act Agreement,* HUMAN RIGHTS WATCH (Oct. 29, 2019, 9:00 AM), https://www.hrw.org/news/2019/10/29/groups-urge-congress-oppose-us-uk-cloud-act-agreement#.

[104] *Id.*

[105] *See* Jennifer Daskal & Peter Swire, *The U.K. – U.S. CLOUD Act Agreement is Finally Here, Containing New Safeguards*, LAWFARE (Oct. 8, 2019, 2:33 PM), https://www.lawfareblog.com/uk-us-cloud-act-agreement-finally-here-containing-new-safeguards.

[106] *Groups Urge Congress to Oppose US-UK Cloud Act Agreement*, *supra* note 103.

[107] *See* Brown, *supra* note 80.

[108] *Id.*

[109] *See Who We Are*, ORG. FOR ECON. COOP. AND DEV., https://www.oecd.org/about/ (last visited Oct. 23, 2021) [hereinafter "OECD"]; OECD, THE OECD PRIVACY FRAMEWORK, 39, (2013).

[110] OECD, THE OECD PRIVACY FRAMEWORK, 16 (2013).

[111] *Id.*

[112] *Id.*

[113] *Id.* at 17.

important step towards interoperability."[114] Global interoperability can "simplify compliance" and "ensure that privacy requirements are maintained."[115]

2. Regional Laws

As a regional law, the EU General Data Protection Regulation ("GDPR") governs over 20 countries - both the European Union member states and the nations of the European Area ("EEA") - and is one of the strictest privacy and security laws in the world.[116] By enacting the GDPR, the EU and EEA have chosen to prioritize the privacy rights of their citizens while working internationally across all levels of government to protect their residents' data.[117] The GDPR governs to two types of entities that handle the personal data of EU citizens or residents: they are called "Processors" and "Controllers."[118]

Processors are a "natural or legal person, or other body" which processes personal data.[119] The type of information protected includes, "personal data in the context of the activities of an establishment of a controller or processor in the Union."[120] The processing of EU subjects' personal data, "offer[ing] goods or services to data subjects in the Union," monitoring data subjects in the Union and processing personal data by a controller not established as part of the Union are all acts governed by the GDPR.[121] A processor that is governed by the GDPR signs a contract under the union or member state law, which binds the processor to standards of the types of data it may process, the duration of processing, and the permitted purposes for processing personal data.[122]

The GDPR defines a Controller to mean a natural or legal person or other body that "determines the purposes and means of the processing of personal data."[123] The Controller's obligations include implementing appropriate safeguards or protection policies to protect personal data.[124] For those who do not comply, the GDPR levies harsh fines, which include flat line fees, or a fine based on four percent of global annual revenue.[125]

The GDPR imposes a duty on businesses that handle any EU resident's personal information to implement "appropriate technical and organizational measures."[126] Technical measures can include things such as firewalls, malware scans, anti-virus protection, two-

---

[114] *Id.* at 33.

[115] *Id.* at 34.

[116] *What is GDPR, the EU's New Data Protection Law?*, GDPR EU, https://gdpr.eu/what-is-gdpr/ (last visited Sept. 10, 2021).

[117] *Id.*

[118] Commission Regulation 2016/679 O.J. (L. 119) 1 (EC).

[119] Commission Regulation 2016/679 O.J. (L. 119) 1, 8 (EC).

[120] Commission Regulation 2016/679 O.J. (L. 119) 1, 4 (EC); *Does the GDPR apply to companies outside the EU?*, GDPR EU, https://gdpr.eu/companies-outside-of-europe/ (last visited Nov. 10, 2021).

[121] *Id.*

[122] *See* Commission Regulation 2016/679 O.J. (L. 119) 1, 49 (EC).

[123] Commission Regulation 2016/679 O.J. (L. 119) 1, 8 (EC).

[124] *See* Commission Regulation 2016/679 O.J. (L. 119) 1, 46 (EC).

[125] *See* GDPR EU *supra* note 116.

[126] *Id.*

factor authentication, or limiting employee access to personal information.[127] The GDPR only allows the processing of personal data in six circumstances:

> (1) the data subject gave specific unambiguous consent to process data, (2) processing is necessary to execute or to prepare to enter into a contract to which the data subject is a party, (3) must process the data to comply with a legal obligation, (4) data process necessary to save someone's life, (5) processing is necessary to perform a task in the public interest or in an official function, or (6) there is a legitimate interest to process someone's personal data.[128]

One of the best known breaches of their duty to establish adequate security measures pursuant to the GDPR is Marriott, which resulted in a large fine over a data breach in 2018.[129] The data breach included "guests' names, email addresses, phone numbers, unencrypted phone numbers, arrival departure information, and guests' VIP status and loyalty program membership number."[130] The Information Commissioner's Office ("ICO") originally threatened a €100 million fine in July 2019, but because Marriott took reasonable steps to mitigate the effects of the breach, the ICO lowered the fine to €18.4 million.[131] Amazon suffered a fine of $877 million dollars regarding the collection of visitors' information when they enter the company's website.[132] Google was fined $56.6 million for failing to provide notice to its users about how Google requests their consent.[133] The largest fine to date is a two hundred and ten million euro fine for the breach of the GDPR and the e-Privacy Directive against Google and Facebook.[134] The fine, implemented by the Commission Nationale de l'Informatique et des Libertés, is for "breaches of laws on cookie use and tracking of user online activity."[135]

---

[127] *See* Elisavet Dravalou, *What "technical and organizational measures" Actually Means*, DPORGANIZER, (Feb. 1, 2021), https://www.dporganizer.com/blog/privacy-management/technical-organisational-measures/. *See also* GDPR EU, *supra* note 116.

[128] GDPR EU, *supra* note 116.

[129] *See* Carly Page, *Marriot Hit With €18.4 Million GDPR Fine Over Massive 2018 Data Breach*, FORBES, (Oct. 30, 2020), https://www.forbes.com/sites/carlypage/2020/10/30/marriott-hit-with-184-million-gdpr-fine-over-massive-2018-data-breach/?sh=60eb437fe4b0.

[130] *Id.*

[131] *See id.*

[132] *See 20 Biggest GDPR Fines of 2019, 2020, and 2021 (So Far)*, TESSIAN (Sept. 6, 2021), https://www.tessian.com/blog/biggest-gdpr-fines-2020/.

[133] *See id.*

[134] Rafi Azim-Khan, *Record €210 Million in Fines for Breach of Cookies and Website Tracking Rules – Note e-Privacy Directive, Not Just GDPR*, JD SUPRA (Jan. 10, 2022), https://www.jdsupra.com/legalnews/record-eur210-million-in-fines-for-2973609/ (last visited Apr. 14, 2022). *See Principle (e): Storage Limitation*, INFO. COMM'RS OFF., https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/principles/storage-limitation/ (last visited Nov. 10, 2021).

[135] Rafi Azim-Khan, *supra* note 134.

3. Individual State Statutory Scheme of Budapest Member States: The United States and China

Unlike Europe, the United States has no "comprehensive general privacy legislation."[136] The United States favors cyberspace regulations created by the private sector; meaning the government only steps in when there are events that affect its citizens.[137] In 2016, the FTC released a guide for businesses instructing them how to protect their personal information.[138] This guide, titled *Federal Trade Commission Privacy and Data Security Update*, is updated annually.[139] The FTC imposes various duties on companies such as assess the information a company possesses, inventory of all devices that contain sensitive data, track personal information through multiple departments, create physical, technological, and administrative safeguards, and institute policies for responding to security incidents.[140]

Where a company fails to comply with its FTC requirements, the Federal Trade Commission Act authorizes preliminary and permanent injunctions to remedy the violation and, in some cases, receive civil penalties.[141] Between 2019 and 2020, some notable FTC cases and proceedings include Facebook, Inc.,[142] Kohl's Department Stores, Inc.,[143] Google LLC and YouTube LLC,[144] Equifax, Inc.,[145] and formerly known app Musical.ly, which is now known as "TikTok."[146]

Legislation such as the Gramm-Leach-Bliley Act ("GBLA") applies to financial institutions and requires them to create privacy policies and safeguards to protect financial and identification information.[147] As part of the GBLA, the covered entities must "develop a written information security plan that describes their program to protect customer

---

[136] FED. TRADE COMM'N, *Federal Trade Commission 2020 Privacy and Data Security Update*, 1, (2020).

[137] *See* Summer Walker, *Cyber-Insecurities?: A guide to the UN cybercrime debate*, GLOBAL INITIATIVE, (Mar. 2019), https://globalinitiative.net/wp-content/uploads/2019/03/TGIATOC-Report-Cybercrime-in-the-UN-01Mar1510-Web.pdf.

[138] *See A Guide for Business: Protecting Personal Information*, FEDERAL TRADE COMM'N (Oct. 2016), https://www.ftc.gov/system/files/documents/plain-language/pdf-0136_proteting-personal-information.pdf.

[139] FED. TRADE COMM'N, *supra* note 136.

[140] *See A Guide for Business: Protecting Personal Information*, *supra* note 138.

[141] *See* Federal Trade Commission Act, ch. 311, 38 Stat. 717; 15 U.S.C. § 53(b); 15 U.S.C. § 45(l).

[142] *FTC Alleges Facebook Resorted to Illegal Buy-or-Bury Scheme to Crush Competition After String of Failed Attempts to Innovate*, FED. TRADE COMM'N (Aug. 19, 2021), https://www.ftc.gov/news-events/press-releases/2021/08/ftc-alleges-facebook-resorted-illegal-buy-or-bury-scheme-crush; *Cases and Proceedings*, FED. TRADE COMM'N, https://www.ftc.gov/enforcement/cases-proceedings (last visited Nov. 10, 2021).

[143] *See Khol's Department Stores, Inc.*, FED. TRADE COMM'N (June 10, 2020), https://www.ftc.gov/enforcement/cases-proceedings/182-3200/kohls-department-stores-inc. *See also Cases and Proceedings*, *supra* note 142.

[144] *See Google LLC and Youtube, LLC*, FED. TRADE COMM'N (Sept. 4, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3083/google-llc-youtube-llc. *See also Cases and Proceedings*, *supra* note 142.

[145] *See Equifax, Inc.*, FED. TRADE COMM'N (July 31, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3203/equifax-inc; *Cases and Proceedings*, *supra* note 142.

[146] *See Musical.ly, Inc.*, FED. TRADE COMM'N (Feb. 27, 2019), https://www.ftc.gov/enforcement/cases-proceedings/172-3004/musically-inc; *Cases and Proceedings*, *supra* note 142.

[147] Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338; 15 U.S.C.S. § 6801 (1999). *See also About the GLB Act*, FED. TRADE COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/how-comply-privacy-consumer-financial-information-rule-gramm (last visited Sept. 24, 2021).

information."[148] The federal government requires the businesses to make the policies and procedures pursuant to the entity's "size, nature and scope" of the activities they conduct, and the sensitivity of the information that it "collects, maintains, and processes."[149] The FTC requires companies to designate an employee to create policy and procedures for the business; identify and assess the risk within their systems and networks; design a safeguard program, regularly test, and update the program; and select to work with providers that also use appropriate safeguards.[150] The GBLA further imposes a duty on the financial institution to provide "clear and conspicuous" written notice of their policies and practices to customers.[151] The GBLA imposes duties on organizations to cooperate and create solutions to data protection breaches.[152] This structure is called the "Multi-stakeholder model," in which primary stakeholders work together to create solutions.[153] This approach promotes collaboration between private and public entities to work together to combat the increasing cyber threats.[154]

China takes a very different approach.[155] China's government takes a hands-on approach in controlling and maintaining the flow of information across and outside of its sovereign territory.[156] Beijing has laid out four goals: (1) "to maintain and control the flow of information to ensure domestic stability, regime legitimacy, and the continued rule of the Chinese Communist Party," (2) to reduce "vulnerabilities in critical networks and defend the country against a range of cyber operations", (3) to ensure "technological autonomy," and (4) to expand their impact in cyberspace and limit the movement of the U.S. and its alliances.[157] China has attempted to control access to the internet since at least 1998.[158] The project referred to as the "Golden Shield Project" or the "Great Firewall of China" was China's attempts to monitor and censor what was allowed to be seen, and what was forbidden to be seen on a Chinese network.[159] China uses various methods to block its citizens from accessing specific websites.[160] Such tactics include "IP blocking, packet filtering, credit records, speech,

---

[148] Gramm-Leach-Bliley Act, Pub. L. 106-102, 113 Stat. 1338; *Financial Institutions and Customer Information: Complying with the Safeguards Rule*, FED. TRADE. COMM'N, https://www.ftc.gov/tips-advice/business-center/guidance/financial-institutions-customer-information-complying (last visited Jan. 21, 2022).

[149] *Id.*

[150] *Id.*

[151] *About the GLB Act*, *supra* note 147.

[152] *See* Walker, *supra* note 137.

[153] *Internet Governance – Why the Multistakeholder Approach Works*, INTERNET SOCIETY, (Apr. 26, 2016), https://www.internetsociety.org/resources/doc/2016/internet-governance-why-the-multistakeholder-approach-works/ (last visited Apr. 13, 2022).

[154] *See* SEOHYUN BAE ET AL., EVOLVING US CYBERSECURITY POLICY: A MULTI-STAKEHOLDER APPROACH 114 (Mayowa Aina & Estella Jung eds. 2016).

[155] *See* Walker *supra* note 137.

[156] *See* Adam Segal, *China's Alternative Cyber Governance Regime*, U.S.-CHINA ECONOMIC AND SEC. R. COMM'N (Mar. 13, 2020), https://www.uscc.gov/sites/default/files/testimonies/March%2013%20Hearing_Panel%203_Adam%20Segal%20CFR.pdf.

[157] *Id.*

[158] *See* Jack Wagner, *China' Cybersecurity Law: What You Need to Know* (June 1, 2017), https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/.

[159] *Free Speech vs. Maintaining Social Cohesion*, STANFORD UNIV., https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreeExpressionVsSocialCohesion/china_policy.html (last visited Jan. 18, 2022).

[160] *See id.*

and facial recognition."[161] China envisions a world in which the national internet is government controlled, maintained and monitored, which is a stark difference from what western countries like the U.S. support.[162]

B. What is the Proposed U.N. Treaty Attempting to Accomplish?

Russia proposed the United Nations Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes.[163] Russia submitted it as a resolution in December 2019.[164] China and Cambodia later joined the proposal as co-sponsors.[165] These states aim to monitor users for stricter government control.[166]The treaty was then drafted by an "intergovernmental expert group (IEG), which conducted a comprehensive study of issues regarding international cybercrime.[167] The study went on for three years starting in 2018.[168]

The proposed treaty aims to criminalize and establish liability for:

> [U]nauthorized access to electronic information, unauthorized interception, unauthorized interference with digital information, disruption of information, creation and distribution of malware, unauthorized interference with information infrastructures, unauthorized access to personal data, unauthorized trafficking in devices, creation of data to mislead the user, incitement of armed activities, terrorism-related offenses, and extremism-related offenses.[169]

The primary goal is to update the 21-year-old cybercrime agreement since our technology has improved and the accessibility to technology has greatly expanded.[170] One section Russia believed needed to be expanded upon was the list of cybercrimes.[171] The Budapest Convention criminalizes 9 actions, and the Russian proposed treaty aims to expand

---

[161] *Id. See generally* Chris Hoffman, *How the "Great Firewall of China" Works to Censor China's Internet,* HOW-TO GEEK (Sept. 17, 2017, 11:23 AM), https://www.howtogeek.com/162092/htg-explains-how-the-great-firewall-of-china-works/ (IP blocking restricts access to certain IP addresses. Filtering packets look for sensitive content and monitor the network for sensitive content coming in or going out of the network.).

[162] *See* Segal, *supra* note 156.

[163] G.A. Res. A/74/401 at 1 (Oct. 11, 2019).

[164] *Id.*

[165] Brown, *supra* note 80.

[166] *See id.*

[167] *Time to Engage: The UN Wades into Global Cybercrime Treaty Debate*, GLOBAL INITIATIVE (May 7, 2021), https://globalinitiative.net/analysis/un-cybercrime-treaty-debate/.

[168] *See id.*

[169] U.N. Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes, Art. 5-30, (July 29, 2021) [hereinafter U.N. Convention on Countering the Use of Info].

[170] *See* Amann Ahmed, *Proposal to the UN for Expanding List of Designated Cybercrimes*, FIRSTPOST (July 28, 2021), https://www.firstpost.com/tech/news-analysis/explained-russias-proposal-to-the-un-for-expanding-list-of-designated-cybercrimes-9843901.html.

[171] *See id.*

the acts prohibited to 23 acts that constitute criminal conduct.[172] The other goal is to "prevent, detect and suppress more effectively" international transfer of information to strengthen international cooperation.[173]

The United States does not support the treaty. The United States has taken a major stand before the UN, "adopting this resolution will drive a wedge between Member States and will undermine international cooperation to combat cybercrime...Instead of adopting this very problematic resolution, Member States should give the Expert group time to complete its work."[174] The reasons for the US voting ageist the resolution are because there is "no consensus among the Member States on the need or value of drafting a new treaty," the resolution "is not based on empirical information," and "the resolution is premature and prejudges the outcome of the existing work of the Expert Group."[175] The free world has argued that the punishing the "incitement of armed activities, terrorism-related offenses, and extremism-related offenses" are meant to heavily censor the internet.[176] By criminalizing these activities, critics assert governments can restrict the freedom of speech and expression on the internet.[177] Others argue that by co-authoring the convention, Russia and China aim to push their authoritarian rules and norms on an international sphere.[178] Article 33 of the proposal exemplifies this, in which, upon signing, each State party must collect or record information and communication technologies ("ICT").[179] Meaning that if nation-states do not currently have legislation that requires the collection of this data, they are required to adopt such measures to preserve the ICT.[180]

C. What obligations does the proposed treaty place on companies, organizations, and other legal persons?

Article 42 of the Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes imposes its duties and sanctions onto the private sector.[181] "Failure to promote the standards and procedures to ensure information security, promote training programs for law enforcement, investigative, judicial or

---

[172] Convention on Cybercrime, art. 2-11, Nov. 23, 2001, ETS 185, T.I.A.S. No. 13174.; U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 6-28.

[173] *Id.* at Preamble.

[174] Jason Mack, *Statement of Agenda Item 107 'Countering the Use of Information and Communications Technologies for Criminal Purposes'*, U.S. MISSION TO THE U.N. (Nov. 18, 2019), https://usun.usmission.gov/statement-on-agenda-item-107-countering-the-use-of-information-and-communications-technologies-for-criminal-purposes/ (last visited Apr. 13, 2022).

[175] *Id.*

[176] Justin Sherman & Mark Raymond, *The U.N. passed a Russia-backed cybercrime resolution. That is not good news for internet freedom*, WASHINGTON POST (Nov. 19, 2018) https://www.washingtonpost.com/politics/2019/12/04/un-passed-russia-backed-cybercrime-resolution-thats-not-good-news-internet-freedom/ (last visited Apr. 13, 2022).

[177] *See id.*

[178] *See id.*

[179] U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 33.

[180] *See id.*

[181] *See generally id.*, at Art. 42 (The primary purpose for including the private sector was to "enhance information security standards" and to hopefully dissuade companies and businesses from violating the treaty by imposing sanctions).

prosecutorial officials, and promote cooperation between law enforcement and the relevant private entities will result in civil and/or criminal sanctions."[182] The States that adopt the convention must enact legislation that empowers authorities to collect or record information by means of information and communication technologies (ICT).[183] Member states must also enact legislation that allows a service provider to collect or record electronic information, including data, which is then transmitted through means of ICT.[184] The treaty further orders "relevant private entities" to cooperate with authorities of that state.[185] The obligation falls onto the state to collect, record and store the data, but entities must provide the information to the state and are required to provide any information if asked by a service provider.[186] Under the terms of the treaty, the government of the signatory states may collect or record the traffic data associated with ICT and bind the service providers to collect and record electronic information or cooperate and assist authorities.[187]

1. Impact on Businesses

Other than governments, the most affected entities will be businesses which would be required to collect, maintain, and report data if the proposal is signed into law.[188] Pursuant to article 34 of the proposal, legal persons must preserve electronic information, preserve the stored information for a set period, and may disclose the data to authorities in the instance of such information if necessary.[189] The proposal is unclear what falls under "specified electronic information," it merely lays out that the type of information that should be preserved is data that is "vulnerable to deletion, copying, or modification."[190] With the broad strokes of the proposal, without further information, this may mean that businesses must collect, maintain, and protect much larger quantities of information than they have previously.[191] The FTC and the GDPR recommends to only collect and retain information unless it is necessary for the service or product and should only be kept as long as need be.[192] Not only will businesses be required to store more information, but in aid of an investigation, their devices containing data affected by a breach of cyber security may be confiscated in the investigation of criminal charges.[193] In which case, the business or entity will need to have a

[182] *Id.*

[183] *Id.*

[184] *See id.*

[185] *Id.*

[186] *See id.*, at Art. 32.

[187] *See id.* at Art. 33.

[188] *See id*, at Art. 34.

[189] *Id.*

[190] *Id.*

[191] *See generally id.*, at Art. 4 (The purpose of the proposal is to protect "information and communication technologies" which includes the "processes and methods of generating, processing, and distributing information, as well as ways and means of their implementation).

[192] *Protecting Personal Information: A Guide for Business, supra* note 138. S*ee Principle (e): Storage Limitation, supra* note 134.

[193] *See* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 70.

plan if their devices and storage is taken for a formal investigation by authorities.[194] Article 73 provides a remedy to return the property, however, the state has the authority to determine whether to return the property or pay compensation to the victims of the cybercrime.[195] The proposal fails to provide a timeline for when the investigative body must return property to companies and does not provide any guidance for the maximum duration that the investigative body can withhold a device or company's information.[196] Without further guidance, a State party may hold the confiscated property for as long as they please, and even then, the property need not be returned to the legitimate owner.[197]

The other impact on businesses is that the treaty fails to provide any explanation for businesses functioning in a state that had not ratified the treaty but does business in a member state.[198] The GDPR lays out that any business that processes and controls data of an EU citizen must abide by the GDPR whether or not they are located within the EU.[199] If, like the GDPR, the treaty requires all businesses that processes, maintains, or distributes ICT to follow the proscriptions of the treaty then almost all international businesses may end up bound by the treaty.[200] However, based on Russia's proposal it is unclear how far the private sector provision extends beyond the individual signatory states.[201]

2. Impact on State Parties

While the proposal places obligations and regulations on State parties, the business entities are also impacted as the State must make policies that require businesses to strengthen their processes and methods of generating, processing, and distributing information as well as training personnel to prevent, detect and investigate ICT crimes.[202] The proposal requires State parties to create plans to "combat ICT crimes, train staff in preparation of request for extradition, create methods to protect victims, train staff in both domestic and international regulations and provide language training."[203] While the State parties will have to figure out a way to implement these changes, businesses in the signatory states must comply with the standard or face fines for violating the international regulations.[204] The businesses must train or hire staff that will attend the training, will help implement the training into their workforce,

---

[194] *See generally id.* (A "state party shall take measures to identify or seize property obtained as a result of the commission of offenses in accordance with the instrumentalities." In this case, a business may not have access to the confiscated device).

[195] *See id.*, at Art. 73.

[196] *Id.*

[197] *Id.*

[198] *See id*, at Art. 42.

[199] GDPR EU, *supra* note 120.

[200] *See generally* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 42; GDPR EU, *supra* note 120 (Applying the GDPR provisions of who it applies to, businesses that conduct business in Russia, China, or any state member that ratifies and processes, distributes, and maintains information of citizens of those states most international businesses may end up bound by the law and required to follow the obligations set forth by the treaty).

[201] U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 42.

[202] *See id.*, at Arts. 75-76.

[203] *See id.*, at Art. 76.

[204] *See id.*, at Arts. 5 & 76.

and will be in charge of preventing and detecting ICT crimes.[205] If there already is staff in place to attend training and implement them into the business, the business is responsible for providing "language training."[206] The proposal is unclear whether the "language training" it will require is referring to different languages such as Arabic, Chinese, Russian, and Spanish or if it is referring to training in the jargon of ICT and breaches to personal information.[207]

The proposal also requires the promotion of raising public awareness of cybercrime prevention, which includes creating easy access to information, zero tolerance of offenses and the creation of public training programs on cyber security.[208] The implication of these requirements includes hiring individuals in charge of creating and maintaining websites with up-to-date information for the public, which is similar to existing positions in the U.S. called Certified Information Security Managers.[209]

D. What are the privacy concerns that the proposed treaty presents?

One concern is the length of the retention period.[210] The ICO addressed the retention period.[211] The GDPR does not have a firm limit on how long a business may store personal data.[212] However, the longer a business has the information stored online, the greater the risk of misuse or mistake.[213] The Russia proposal does not provide a specific time for data retention, rather, it allows the domestic or regional laws to maintain the timing requirements.[214] Companies will have to stay up to date with various state and regional laws to ensure they comply with Russia's proposed treaty.[215]

Another concern of the free world is the transmission of data across borders for the "purposes of criminal, administrative, or civil proceedings."[216] The cause of concern is that "[p]ersonal data transmitted from one State party to another State party at the request made in accordance with the convention may be used by the State party," for the purposes of the abovementioned proceedings.[217] If the State party is giving the consent to another State party, the proposal fails to provide guidance for notifying the victim whose private personal information was misused or accessed and will be shared with the investigating State party.[218] The draft further explains that states may not share personal data with a third party without

---

[205] *See* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 76.

[206] *See id.*

[207] *See id.*

[208] *See id.*, at Art. 44.

[209] Steve Morgan, *Cybersecurity Jobs Report: 3.5 million Openings in 2025*, Cybercrime Magazine, (Nov. 9, 2021), https://cybersecurityventures.com/jobs/ (last visited Apr. 13, 2022).

[210] *See* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 34; *see* INFO. COMM'RS. OFF., *supra* note 134.

[211] INFO. COMM'RS. OFF., *supra* note 134.

[212] *See id.*

[213] *See id.*

[214] U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 34(2).

[215] *Id.*

[216] *Id.*, at Art. 56.

[217] *Id.*

[218] *Id.*

consent of the State party.[219] One of the Convention's aims is to protect "civil society," which includes individuals within the signatory's territory.[220] Yet the draft does not address the victims of ICT crimes and allows the State party to consent to the sharing of the victims' private personal information without their knowledge.[221]

Last, the two portions criminalizing "terrorism-related offenses" and "extremism-related offenses" are two points of contention.[222] "Terrorism-related offenses" is a broad phrase, and the proposal gives little information on what constitutes such acts.[223] China has implemented Counterterrorism laws, which also do not clearly articulate "terrorism" and "extremism," but allow the government to criminalize speech that "incites criminal acts" or intends to result in criminal action.[224] By having such expansive language, it provides access for authoritative governments to closely monitor their members and suppress their freedom of speech to forbid criticism.[225] These articles conflict with the United States Constitution and the values that the United States was founded upon, therefore as it stands, these amendments alone would be cause for the U.S. and many other countries to decline to sign the treaty.[226]

IV. SOLUTION

A. What parts of the Cybercrime convention are still relevant today?

The Council of Europe Convention on Cybercrime is still relevant as it prohibits cyber-related crimes and aims to harmonize national cybercrime laws.[227] In fact, the Council of Europe Convention on Cybercrime is still the governing treaty regarding cybercrime in the signatory countries.[228] Cybercrime has continued to plague the internet, which has caused the pressure to update the international cybercrime laws to link states together to fight against cybercrime.[229] Unfortunately, during the Covid-19 pandemic, millions of dollars were ransomed by cybercriminals.[230] Officials have recognized that cybercrime continues to grow

---

[219] *Id.*

[220] *Id.* at Preamble.

[221] *Id.* at Art. 56.

[222] *Id.* at Arts. 20-21; Sherman & Raymond *supra* note 176.

[223] *See* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 20.

[224] *China: Disclose Details of Terrorism Convictions: Overbroad Counterterrorism Legal Framework Opens Door to Abuses,* HUMAN RIGHTS WATCH, (Mar. 16, 2017), https://www.hrw.org/news/2017/03/16/china-disclose-details-terrorism-convictions.

[225] *Id*; *See* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 20.

[226] U.S. Const. amend. I.

[227] Daskal & Kennedy-Mayo *supra* note 75.

[228] *See generally Parties/Observers to the Budapest Convention and Observer Organisation to the T-CY, supra* note 74 (All of the member countries are still active under the treaty and none of the member states have not withdrawn from the Budapest Convention, therefore as the Budapest Convention is still good law, all member states are bound).

[229] *Id.*

[230] Dan Patterson, *Cybercrime is Thriving During the Pandemic Driven by surge in Phishing and Ransomware,* CBS NEWS (May 19, 2021, 11:20 AM), https://www.cbsnews.com/news/ransomware-phishing-cybercrime-pandemic/.

and targets all groups of people amassing money from these attacks.[231] The Russian proposal includes and expands upon most if not all the crimes that were originally included within the Budapest Convention. [232] Therefore, the parties to the Budapest Convention, may bring charges against cybercriminals under the treaty, but they must fall within the specified nine charges.[233] While there is currently not a court, the principle on territorial jurisdiction stems from the *Lotus* case in which the Permanent Court of International Justice laid out that a state cannot exercise its jurisdiction outside its territory, unless an international treaty allows it to do so.[234] Thus, with a limited scope of the treaty may allow the Member State where the crime occurred to prosecute the cybercriminal.[235]

B. What are some parts of the proposed treaty that may be beneficial?

When the Convention on Cybercrime was written, cloud data storage, and electronic storage of information were not taken into consideration in the drafting of the treaty.[236] The proposed Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes fills these gaps, to protect the information on these systems and criminalize those that aim to exploit them.[237] Expanding the scope of criminal conduct is beneficial, at least to a certain extent because, as technology has grown, the types of hacking and the manner of hacking have developed in conjunction.[238] For example, Internet communication and technology-related theft is much more broad than the prohibition of theft of property through means of destruction, modification, blocking or copying data with ICT operations.[239] The Convention on Cybercrime only mentions illegal access and interception, data interference, system interference and misuse of devices, and computer forgery and fraud, which leads to broad interpretations and inconsistent determinations.[240]

C. Addressing Privacy Concerns with Russia's Proposal

The storage of data is necessary for the business to conduct its activity but may also be necessary for discovery.[241] What the experts, state policymakers, and third parties will

---

[231] *See* Allison Peters & Anisha Hindocha, *US Global Cybercrime Cooperation: A Brief Explainer*, THIRD WAY (June 26, 2020), https://www.thirdway.org/memo/us-global-cybercrime-cooperation-a-brief-explainer (last visited Apr. 13, 2022).

[232] Convention on Cybercrime, art. 2-11, Nov. 23, 2001, ETS 185; U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 6-30.

[233] Convention on Cybercrime, art. 2-11, Nov. 23, 2001, ETS 185.

[234] S.S. *Lotus* (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

[235] *See generally* S.S. *Lotus* (Fr. v. Turk.), 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7) (Applying the principle laid out by the court, the Member State may have jurisdiction over a cybercriminal in their state if the treaty provides that they may do so).

[236] *Id.*

[237] G.A. Res 75/282 at 3 (May 26, 2021).

[238] G.A. Res 75/282 at 7-12 (May 26, 2021).

[239] G.A. Res 75/282 at 10 ((May 26, 2021).

[240] Convention on Cybercrime, art. 2-8, Nov. 23, 2001, ETS 185, T.I.A.S. No 13174.

[241] Marcus Evans et al., *Record Retention is a Key Component of Your Privacy and Cyber Compliance Program*, NORTON ROSE FULBRIGHT, (Dec. 23, 2019), https://www.dataprotectionreport.com/2019/12/record-retention-is-a-key-component-of-your-privacy-and-cyber-compliance-program/ (last visited Apr. 13, 2022).

need to determine whether they would like to place a specific required retention period.[242] There is merit to the argument that the type of data and the size of the business should be taken into consideration.[243]

By failing to share information across borders about cybersecurity attacks and events, countries will undermine their cybersecurity infrastructures.[244] Sharing the information about the attacks will provide a more efficient remedy and provide information on vulnerabilities and gaps in cybersecurity systems.[245] Since sharing information across borders is necessary for the development in technology and to develop defenses, the challenge to overcome is the state consenting on behalf of their citizens who fell victim to a cyberattack.[246] The way to combat this issue is to provide a notification system to victims to promote transparency with what information is shared, to whom their information is shared, and where to access information regarding the cyber event.[247]

The criminalization of terrorism and extremism related offenses are broad and undefined within the Russia proposal.[248] The concerns with such a proposal are that it would overstep onto the freedom of speech and the punishment.[249] It is unlikely that the U.S. and other major countries will sign the proposal unless during negotiations specific sections are removed, or the definition of "terrorism-related offenses" and "extremism related offenses" is so narrowly tailored that it may only criminalize specific acts and it cannot be abused.[250]

D. An Acceptable Solution

The US should push for a new treaty to be drafted or for the Russia proposal to be amended.[251] It is highly unlikely that the United States and other democracies will sign the proposed Russian and Chinese treaty.[252] However, as negotiations occur, amendments should be proposed, or a proposal for a new cybercrime treaty to be drafted to address the changes in

---

[242] *See id.* (Data is not just a risk but rather a crucial aspect of a business. State governments have long recommended that companies properly dispose of information at the time it is no longer necessary to retain it. It should be discussed whether a set of data would be beneficial, or tailoring based on size).

[243] *See id.* (Not all data is the same and should not be treated as such to promote the use of a blanket retention period).

[244] Nigel Cory and Luke Dascoli, *How Barriers to Cross-Border Data Flows are Spreading Globally, What they Cost, and How to Address Them*, INFORMATION TECHNOLOGY & INNOVATION FOUNDATION, (July 19, 2021), https://itif.org/publications/2021/07/19/how-barriers-cross-border-data-flows-are-spreading-globally-what-they-cost (last visited Apr. 13, 2022).

[245] *Id.*

[246] *Id.*; U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 56.

[247] *See generally* Commission Regulation 2016/679 O.J. (L. 119) 1 (EC). (The GDPR provides a similar requirement within their regional cybersecurity law. The GDPR provides individuals with the right to be informed. The requirements include making sure that individuals are made aware of the processing of their personal data and how to exercise their rights).

[248] U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 20-21.

[249] *See id.*, at Art. 20; *see* HUMAN RIGHTS WATCH, *supra* note 224.

[250] *See* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 20; Brown, *supra* note 80.

[251] Kevin Lynch, *Cybersecurity is a Global Problem, So Where's the Global Response?*, FORBES (May 20, 2021), https://www.forbes.com/sites/forbestechcouncil/2021/05/20/cybersecurity-is-a-global-problem-so-where-s-the-global-response/?sh=16b403785e41.

[252] Brown, *supra* note 80.

technology over time should be brought to the table.[253] Democracies, not just authoritarian states such as Russia and China, should send their cyber experts, diplomats, and business shareholders to the negotiating table.[254] If businesses are to be bound and even sanctioned under the terms of the treaty, or the legislation enacted thereunder, then businesses should be consulted on and participate in the drafting of the treaty provisions.[255] Businesses like Google, Amazon and Marriott, that have a high possibility of receiving fines should weigh in.[256] In the drafting, a committee should consult businesses that conduct businesses worldwide; they will provide insight to help create a policy that mitigates risks,[257] explain how strict policies may impact businesses both small and large, and provide input on the costs incurred if they do not properly protect private information.[258] Small businesses are targets for cyber-attacks and most likely have the least amount of resources to address a cyber event.[259] Since small businesses typically lack security infrastructure and are easy targets for hackers, policy makers should also take into account these businesses when creating binding policies for businesses.[260]

The definition of cybercrime needs to be broadened to include a more expansive version of what is protected and what is criminalized, as reflected in the most recent proposal.[261] While the Supreme Court of the United States has defined "excess unauthorized use," the decision is not binding on other nation states.[262] Because many states have tailored the Budapest Convention to their state laws, a new cybercrime treaty can use the Expert Group's research based on empirical data to formulate a supported definition.[263] However, Russia's proposed treaty has included other criminal offenses that expand upon the Budapest Convention which have accounted for the changes and access to technology.[264] For example, the treaty criminalizes "disruption of information and communications networks," "unauthorized trafficking in devices," and "ICT related theft" but only requires each State party to recognize the offense without defining what acts fall within each article.[265]

The treaty should take the GDPR into consideration.[266] It lays out comprehensive data protection principles that may be applicable and imposes policies on private entities to

---

[253] *See* Daskal & Kennedy-Mayo, *supra* note 75.

[254] Sherman & Raymond, *supra* note 176.

[255] *See generally* U.N. Convention on Countering the Use of Info, *supra* note 169, at Art. 42 (If the drafters of the treaty aim to include a private sector provision, such as article 42 in Russia's proposal, any business in a member state that sign's this treaty will be bound to its proscriptions.)

[256] Page, *supra* note 129.

[257] *The 4 Most Important Cyber Security Policies for Businesses*, GRAY ANALYTICS, (May 21, 2021), https://www.grayanalytics.com/blog/the-4-most-important-cyber-security-policies-for-businesses/ (last visited Apr. 13, 2022).

[258] Abi Tyas Tunggal, *Why is Cybersecurity Important*, UPGUARD, (Oct. 18, 2021), https://www.upguard.com/blog/cybersecurity-important (last visited Apr. 13, 2022).

[259] *See Stay Safe from Cybersecurity Threats*, U.S. SMALL BUS. ADMIN., https://www.sba.gov/business-guide/manage-your-business/stay-safe-cybersecurity-threats (last visited Jan. 2, 2021).

[260] *See id.*

[261] *See* GDPR EU. *supra* note 116.

[262] Van Buren v. United States, 141 S. Ct. 1648 (U.S. June 3, 2021).

[263] *See* COUNS. OF EUR., *supra* note 86 at 6-7; Jason Mack, *supra* note 174.

[264] U.N. Convention on Countering the Use of Info, *supra* note 169, at Arts. 6-29.

[265] *Id.*, at Arts. 9, 13, and 14.

[266] *See* GDPR EU, *supra* note 116.

ensure the safety of their data, unlike the proposed treaty, which mandates that the state collect the information from private entities.[267] Not only is this putting a lot of responsibility on the state to have secure systems, but it would require a new agency to take all the information and sort through it to organize and file all that it would receive. Further, the drafters should look to the New York law, which requires licensed and registered private entities to file a report when even the possibility of a cyberattack occurs.[268] An international reporting system run by a subdivision of the UN would be beneficial as it would collect the information similar to New York State's Department of Financial Services, but it would create a database that filters the information of type of attack and form of attack for all participating countries to review and use for their investigations into cybercrime.[269] The production of a list of previous attacks or attempted attacks and the form of attack an entity received may allow law enforcement to narrow attacks to individuals or groups.[270]

Drafting a new treaty would fill the gaps that we see in the current cybercrime convention.[271] By drafting a treaty that involves multiple types of entities viewing cybersecurity policies from different perspectives, the treaty will promote working together to combat cybercrime rather than pushing various political agendas.[272] A proposal to remedy this issue is the implementation of a reporting system to share internationally and update frequently, as well as, placing responsibilities on businesses similar to the GBLA or the NYCRR to implement policies and procedures that best protect businesses from cyber-attacks.[273] This ultimately will benefit the efficiency of the investigative response and will ensure organizations implement security measures to protect the consumer or possibly face the consequence of a fine.[274]

V. CONCLUSION

The proposed Convention on Countering the Use of Information and Communications Technologies for Criminal Purposes has too many issues that will result in many countries failing to sign and ratify the treaty due to the ethical and human rights violations.[275] Many forms of legislation regarding cybercrime exist and implement rules that would be beneficial on an international level.[276] By synthesizing several cybercrime laws, nations can more effectively fight against cyber-attacks in a way that is efficient for the

---

[267] *Id.*

[268] Das, *supra* note 61.

[269] *Id.*

[270] *See* Catherine Stupp, *Interpol Aims to Set Up International Cybercrime Database*, WALL STREET JOURNAL, (Oct. 15, 2019), https://www.wsj.com/articles/interpol-aims-to-set-up-international-cybercrime-database-11571131803.

[271] Daskal & Kennedy-Mayo, *supra* note 75.

[272] Sherman & Raymond, *supra* note 176.

[273] *See* Stupp, *supra* note 270; 15 U.S.C. § 6801; 23 NYCRR § 500 (2017).

[274] Das, *supra* note 61; GDPR EU, *supra* note 116.

[275] *See* Sherman & Raymond, *supra* note 176; Brown, *supra* note 80.

[276] Das, *supra* note 61; GDPR EU, *supra* note 116; U.N. Convention on Combating Information Technology Offenses, art. 5-18, (Dec. 21, 2010); African Union Convention on Cyber Security and Personal Data Protection, art. 27 and 29, (May 11, 2020).

businesses involved and for the consumers.[277] By using policies and procedures from different countries' domestic laws and treaties that are known to be effective, the United Nations can create a treaty that accurately reflects the ratifying countries' values, which will ultimately reduce cybercrimes and facilitate international cooperation.[278]

[277] *See* Lynch, *supra* note 251.

[278] UNITED NATIONS OFF. ON DRUGS AND CRIME, *Harmonization of Laws*, https://www.unodc.org/e4j/en/cyber crime/module-3/key-issues/harmonization-of-laws.html (last visited Jan. 19, 2022).