2018

In Defense of the Global Regulation of a “Duty to Report Crime”

Sungyong Kang
Fordham University School of Law

In Defense of the Global Regulation of a "Duty to Report Crime"

Dr. Sungyong Kang†

I. INTRODUCTION

In a previous article, "In Defense of Duty to Report Crime," a normative case was made for domestic "duty to report crime" laws that criminalize certain private actors for their failure to report crimes.[1] The basic point in that article was that such laws are justified under a moral culpability analysis. It was argued there that in some circumstances, an offender,[2] a third-party observer, or even a victim has a strong moral duty to inform the relevant authorities that a potentially criminal act has been committed. In that earlier article, it was also asserted that existing domestic laws that promulgate a "duty to report crime" are justifiable, or can be revised to reflect this normative framework.

This article will build upon the prior analysis of domestic "duty to report crime" laws by describing and analyzing what can be done at the international level with "duty to report crime" laws. The analysis put forward in the previous article is taken as a given, namely, that there is a moral, normative case for "duty to report crime" laws.

This article consists of four parts. Part I sets out the parameters of the problem by employing a hypothetical example which we will return to throughout the analysis in succeeding parts of the paper. Part II discusses the taxonomy of crime with a tripartite classification and then discusses the methods of analysis for analyzing efficiency as well as providing an overview of the inadequacy of the current international regime. Part III sets out a legislative blueprint for the global regulation of a "duty to report

---

† S.J.D., Attorney at Law licensed in New York, Researcher at Police Science Institute (South Korea).
I wish to thank Thomas Lee, Sean Griffith, and Youngjae Lee for their helpful comments to this paper.

1. Dr. Sungyong Kang, *In Defense of Duty to Report Crime*, 86 UMKC L. REV. (forthcoming 2018).

2. *Id.* at 363 ("'Offender-reporter', as used here, means only the person, including a legal entity, with possible strict vicarious criminal liability for such entity, not the person who commits or aids and abets the underlying crime with general criminal liability. To differentiate between these two types of offenders, I use 'Offender' for the former and 'Primary Offender' for the latter. Also, Offender does not include a person who has no liability in relation to the crime committed within their organization. As only the person who can control and oversee the behavior of Primary Offender bears possible strict vicarious criminal liability, a person without such control or oversight will be considered a third party.").

crime" and suggests three key criteria, all of which must be met for global regulation to be effective. Finally, Part IV provides a conclusion and a rationale as to why this legislative blueprint can and should be implemented.

Crimes in the current global-digital era increasingly defy purely domestic "duty to report crime" laws. The characteristics of such crimes are "global-digital" as opposed to "local-physical"; they take the form of multinational networks of criminals exploiting digitalized services of such things as financial institutions and Internet Service Providers ("ISP"), among others.[3] They do this to transport illicit money,[4] child pornography,[5] and private information[6] across national borders, and to incite violence and terrorist acts around the world.[7] Domestic laws and enforcement institutions are quite simply inadequate to detect and deter the full range of global-digital crimes. Moreover, horizontal cooperation at the state-to-state level alone is inadequate in the global-digital context.

To detect, punish, and deter some (or most) crimes in today's era of hyper-globalization and digitization, high degrees of coordination along two dimensions are necessary: both horizontally, state-to-state, and vertically, between state entities and choke point[8] private actors.[9] In this article we shall refer to the combination of these two dimensions as "transnational vertical" cooperation. It is "vertical" insofar as it requires cooperation between choke point private actors who report crime to the state ("bottom-up") and the state to provide the required information to the choke point private actors ("top-down"), which it, in part, acquires from

---

3. *See* Louise I. Shelley, *Crime and Corruption in the Digital Age*, 51 J. OF INT'L AFF. 605, 605 (1998).

4. Luke Harding et al., *British Banks Handled Vast Sums of Laundered Russian Money*, GUARDIAN (Mar. 20 2017), https://www.theguardian.com/world/2017/mar/20/british-banks-handled-vast-sums-of-laundered-russian-money [https://perma.cc/NN9R-TPZX].

5.Anastasia Moloney, *Child Sex Traffickers Turn to Rural Areas, Internet for Business,* REUTERS (Sept. 19, 2017), https://www.reuters.com/article/us-global-slavery-sexcrimes/child-sex-traffickers-turn-to-rural-areas-internet-for-business-idUSKCN1BU25M [https://perma.cc/P9N8-KSZB].

6. Ruby Kitchen & Chris Burn, *Details of a Million People Across Yorkshire for Sale on 'Darkweb'*, YORKSHIRE POST, (July 25, 2017), http://www.yorkshirepost.co.uk/news/details-of-a-million-people-across-yorkshire-for-sale-on-dark-web-1-8668876 [https://perma.cc/SVJ8-QTB9].

7. Michael Jacobson, *Terrorist Financing on the Internet*, 2 CTC SENTINEL 17, 17–20 (2009), https://www.washingtoninstitute.org/uploads/Documents/opeds/4a438817e3a3c.pdf [https://perma.cc/6CTZ-JF7B].

8. The dictionary definition of choke point is "[a] point of congestion or blockage." *Choke Point*, OXFORD LIVING DICTIONARY, https://en.oxforddictionaries.com/definition/choke_point [https://perma.cc/5BDP-BN6Q]. The choke point in this paper refers to a point of blockage to deter crime.

9. This paper generalizes and theorizes the argument made in a prior research paper concerning global regulation of a duty to report suspicious activities imposed on financial institutions to deter corruption and money laundering. *See* Dr. Sungyong Kang, Rethinking the Global Anti-Money Laundering Regulations to Deter Corruption: A Model for Public-Private Cooperation 2 (Feb. 5, 2018) (unpublished manuscript) (on file with the International & Comparative Law Quarterly) ("AML/PEP regulation could avoid, or at least minimize, the collateral damage while maximizing corruption deterrence, if high degrees of coordination along two dimensions were satisfied: the trans-border, and between public enforcement entities and private actors.").

other states.

This article aims to show that "transnational vertical" cooperation is necessary to ensure optimal levels of deterrence for the types of "super" harms that justify domestic laws to criminalize the failure to report crime in the first place, as these harms are increasingly committed in a networked global-digital manner in the modern era. It is not simply a case of doing a "better" job of, for example, deterring corruption or terrorism; this kind of cooperation may even be essential to addressing such harms. A hypothetical example will assist our understanding of the problem.

Two foreign terrorists plan to hijack a flight from Charles de Gaulle Airport in Paris to Kuala Lumpur International Airport in Malaysia, intending to crash the flight into the Stade de France in Saint-Denis during a football match. As they are known foreign terrorists listed on an International Criminal Police Organization ("INTERPOL") database,[10] they buy Austrian and Italian passports stolen in Thailand in 2012 and 2013 on the black market. They open bank accounts with BNP Paribas in Paris using the stolen passports, and their terrorist organization wires money to those accounts to finance aviation school education. On the appointed day of their attack, the foreign terrorists enter Charles de Gaulle Airport, check in for their flight, and pass through the security check. However, at the exit control, the immigration officers disrupt the terrorists' plot and save the lives of hundreds, maybe thousands, of civilians, due to a positive match on INTERPOL's Stolen and Lost Travelling Document ("SLTD") database.[11]

This story is fictional, but many of the details are real and recognizable. In 2001, terrorists with links to Al-Qaeda hijacked four domestic commercial flights and crashed two of those planes into the World Trade Center in New York. In 2015, foreign Islamic State terrorist fighters, who were returning from Syria, carried out suicide bombings and mass shootings in Paris. Furthermore, even though there is no established connection with terrorism,[12] it is well-known that Malaysia Airlines Flight

---

10. *See* Press Release, *Information Sharing is a 'Tripwire' Against Foreign Terrorist Fighters*, INTERPOL (Feb 19, 2015), http://www.interpol.int/News-and-media/News/2015/N2015-015 [https://perma.cc/QM7M-R4VF] ("[C]lose to 40 countries have already provided information to INTERPOL on more than 1,500 suspected and confirmed fighters linked to Syria and Iraq."); *id.* (citing S.C. Res. 2178, ¶ 18 (Sept. 24, 2014)) ("identifying INTERPOL as the 'global law enforcement information sharing' platform against foreign fighters").

11. *See SLTD Database*, INTERPOL, http://www.interpol.int/INTERPOL-expertise/Border-management/SLTD-Database [https://perma.cc/PKB9-AZBT] ("INTERPOL's [SLTD] enables INTERPOL National Central Bureaus (NCBs) and other authorized law enforcement entities—such as immigration and border control officers—to ascertain the validity of a travel document (passports, identity documents, visas) in seconds . . . . Details of stolen and lost passports are submitted directly to the SLTD database by INTERPOL NCBs and law enforcement agencies via INTERPOL's I-24/7 secure global police communication system.").

12. *Malaysia Airlines MH370: Stolen Passports 'No Terror Link'*, BBC (March 11, 2014), http://www.bbc.com/news/world-asia-26525281 [https://perma.cc/H3YC-6HNM].

370, which was scheduled to fly from Kuala Lumpur International Airport in Malaysia to Beijing Capital International Airport in China, disappeared on March 8, 2014. Later, officers discovered that two Iranian men were traveling on that flight with Austrian and Italian passports stolen in Thailand in 2012 and 2013, both of which were registered on INTERPOL's SLTD database.[13] Thus, if frontline officers (in this case, immigration officers) at the border did not have access to such information about stolen passports, which is shared through INTERPOL, the hypothetical example given above could have been a real-life disaster.

Consider digital space, by contrast. There are no territorial and physical borders that frontline law enforcement officers can police. The Internet allows criminals to remotely access and create harm through globally-integrated networks, sometimes even anonymously, regardless of physical borders. Through internationally connected financial services, criminals move illicitly-gained money swiftly from one jurisdiction to another via the Internet. Similarly, when an individual uses an ISP to upload an image located on a server in a foreign state, there is no frontline law enforcement officer monitoring whether the image is, for example, child pornography. The same problem applies to a hacker who sends an email with malware to employees of critical infrastructure in a foreign country.

To detect and deter crime in the global-digital era, states have no choice but to increasingly rely on private sector actors who are often crime victims or facilitators, instead of frontline law enforcement officers. In the hypothetical above, if there were no immigration officers, then states would have to depend on airlines, which provide the travel or financial institutions that transfer the money used to finance crime, to detect and report it to national authorities for further investigation and possible indictment. However, detection and reporting of crime is only possible and feasible if the private sector is equipped with the requisite governmental crime information: both domestic and foreign. In the hypothetical provided above, the frontline law enforcement was authorized to access INTERPOL's SLTD database. If the airline had access to the SLTD database, it could have directly discovered the suspicious identity of the foreign terrorists when they were booking the flight and again when they checked in for the flight. Likewise, if INTERPOL had shared the SLTD database with BNP Paribas, the foreign terrorists might have been exposed to national law enforcement authorities when they attempted to open a bank account.

---

13. Press Release, *INTERPOL Confirms at Least Two Stolen Passports Used by Passengers on Missing Malaysian Airlines Flight 370 Were Registered in its Databases*, INTERPOL (Mar. 9, 2014), http://www.interpol.int/News-and-media/News/2014/N2014-038 [https://perma.cc/HY6D-6CYK].

This sort of transnational vertical cooperation is at an embryonic stage. New top-down cooperation initiatives are showing promise, though they currently depend on voluntary reporting of crime by private actors. For instance, INTERPOL, following a 16-month pilot project with AirAsia, recently endorsed the I-Checkit program.[14] I-Checkit is a border management screening process that gives private actors such as airlines access to its SLTD database, pursuant to a resolution adopted at INTERPOL's 84th General Assembly in 2015.[15] Although I-Checkit is currently the only system that allows direct access by a private sector to crime information possessed by domestic and foreign governments, it should be expanded further, both in scope and content. Eventually, I-Checkit will be piloted in other industries, including the hotel, banking, and maritime transportation sectors.[16]

The importance of international sharing of governmental crime information with the private sector (top-down cooperation) becomes even more critical when states impose a regulatory obligation on the private sector to report (bottom-up cooperation), effectively making the latter take on the role of frontline law enforcement officers.[17] A start in that direction is evident in the United Nations' multilateral treaties that tackle specific transnational crimes, including corruption, terrorism, and drug-trafficking—such conventions typically require member states to impose a duty to report suspicious transactions on their financial institutions.[18] Additionally, to combat cybercrimes, the European Union ("EU") adopted a directive that obligates public electronic communications service providers to report a breach of security that leads to personal data being lost or stolen.[19] It also requires market operators to flag incidents that significantly impact the security of the core services they provide.[20]

---

14. The INTERPOL I-Checkit Solution, AG-2015-RES-03, 1 (2015), https://www.interpol.int/News-and-media/Events/2015/84th-INTERPOL-General-Assembly/84th-INTERPOL-General-Assembly-Resolutions [https://perma.cc/J7J5-9FP6].

15. *See id.*

16. *Id.* at 2.

17. *See Interpol Stolen Passport Database Open to 2 Airlines*, RT (Mar 12, 2014), https://www.rt.com/news/interpol-stolen-passport-database-318/ [https://perma.cc/4SWB-VZFK] (citing the statement of Tony Tyler, Director General of the International Air Transport Association) ("It is not a job for airlines, it is a job for governments.").

18. U.N. Convention Against Transnational Organized Crime, Dec. 13, 2000, 40 I.L.M. 335 (2001) [hereinafter UNTOC]; U.N. Convention on Corruption, Dec. 9, 2003, 43 I.L.M. 37 (2004) [hereinafter UNCAC]; U.N. Convention Against Illicit Traffic in Narcotic Drugs and Psychotropic Substances, Dec. 20, 1988, 28 I.L.M. 493 (1989) [hereinafter UNNDPS]; International Convention on Financing of Terrorism, Dec. 9, 1999, 39 I.L.M. 270 (2000) [hereinafter UNICSFT].

19. Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector, 2002 O.J. (L 201) 37 [hereinafter E-privacy Directive], http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CONSLEG:2002L0058:20091219:EN:HTML [https://perma.cc/67ZT-5CKT].

20. Directive 2016/1148 of the European Parliament and of the Council of 6 July 2016 Concerning Measures for a High Common Level of Security of Network and Information Systems Across the Union, 2016 O.J. (L 194) 1 [hereinafter NIS Directive], http://eur-lex.europa.eu/legal-

However, these global initiatives only impose one-way, bottom-up obligations; they do not emphasize the need for governments to share information with the private sector to enable it to accomplish those obligations in a global, digitized world.

II. IN DEFENSE OF THE GLOBAL REGULATION OF A "DUTY TO REPORT CRIME" IN THE GLOBAL-DIGITAL ERA

In a previous paper, an argument was put forward in favor of making the failure to report certain acts a crime in some domestic contexts.[21] International criminal law is a different enterprise, given the scarcity of international enforcement institutions. The International Criminal Court ("ICC"), for instance, confines its jurisdiction to a small set of the most serious crimes—war crimes, crimes against humanity, genocide, and aggression.

In theory, this small set should be expanded to include other serious offenses, such as terrorism, corruption, international money laundering, or global drug dealing, which are currently entrusted to domestic criminal enforcement. But, consensus is lacking on the question of whether these are international crimes requiring international enforcement.

When we explore the ramifications of a duty-to-report in the international context, we run up against the fact that there is no serious argument favoring an international crime of failure to report. Instead, the international treaties impose a "duty to report crime" but do not specify any penalty for a failure to report crime. For instance, none of the international treaties that impose a duty to report suspicious transactions identify the sanctions for noncompliance. These are the UN Convention against Illicit Traffic in Narcotic Drugs and Psychotropic Substances ("UNNDPS"),[22] the UN International Convention for the Suppression of the Financing of Terrorism ("UNICSFT"),[23] the UN Convention against Transnational Organized Crime ("UNTOC"),[24] and the UN Convention Against Corruption ("UNCAC").[25]

Additionally, the EU directives that impose a duty to report cyber incidents or data breaches do not dictate any specific sanctions for noncompliance. In relation to a duty to report cyber incidents, Article 21 of the Directive of the European Parliament and of the Council Concerning Measures for a High Common Level of Security of Network

---

content/EN/TXT/?uri=uriserv:OJ.L_.2016.194.01.0001.01.ENG&toc=OJ:L:2016:194:TOC [https://perma.cc/54VZ-THG9].

21. Kang, *supra* note 1.
22. UNNDPS, *supra* note 18.
23. UNICSFT, *supra* note 18.
24. UNTOC, *supra* note 18.
25. UNCAC, *supra* note 18.

and Information Systems Across the Union ("NIS Directive") gives discretion to each member state while requiring the sanction to be "effective, proportionate and dissuasive."[26] Regarding failure to report data breaches, Article 15a of the Amended Directive 2002/58/EC of the European Parliament and of the Council of 12 July 2002 Concerning the Processing of Personal Data and the Protection of Privacy in the Electronic Communications Sector ("E-privacy Directive") mentions a criminal penalty but simply as one of the possible sanctions, instead leaving member states to decide the "effective, proportionate and dissuasive" sanction.[27]

Relevant discussion focuses on how to facilitate publicly beneficial acts of reporting crime in the absence of the threat of criminal enforcement. Accordingly, the question reduces to: what can we do to ensure maximum compliance with a "duty to report" when criminal law is not an option?

In this Part, I articulate how this may be done. In doing so, solutions do not appear so much as "criminal law," per se, but rather as "administrative law," or more properly, "global administrative law." The particular type of global administrative regime is perhaps best characterized as a "transnational public-private partnership" ("transnational mutual vertical cooperation"). This regime has certain key features that will be illustrated throughout this Article.

A. Taxonomy of Crime

To establish a basis for further analysis, this Article categorizes the crimes to be reported into three different classifications. This taxonomy of crime is based on the current main modus operandi of the crime. Because the modus operandi of a crime could be diverse or in transition by exploiting the technological development, it is difficult to make a clear-cut classification of a specific crime into one of three types simply by using its legal name. Depending on the modus operandi that is targeted by a duty to report, a crime of terrorism could be transnational-physical (e.g. terrorist bombings) or global-digital (e.g. financing of terrorism). The crime of sexual abuse of a child, which is currently regarded as a local-physical crime, could soon be regarded also as a transnational-physical crime. Nevertheless, a tripartite classification is set out below and the characteristics of each category is briefly described in each of the following three sections.

---

26. NIS Directive, *supra* note 20, art. 21.
27. E-privacy Directive, *supra* note 19, art. 15(a)(1).

1. Local-Physical Crime

Before the development of transportation and telecommunication technologies diversified how criminal purposes could be achieved, crimes tended to be committed physically and locally. For instance, to commit property crimes, criminals had to physically invade someone's property. To commit bodily harm, criminals had to use physical force, sometimes with weapons.

Even in this modern digitalized global era, local-physical crimes make up a large proportion of the total crimes committed. For instance, most crimes against children are committed physically by family members,[28] and sexual abuse of children tends to be committed locally by family members or by people known to the child.[29] Elder abuse is mostly committed in domestic settings (the elder's or caregiver's home) or institutional settings (such as residential facilities for the elderly).[30] In addition, some crimes are local-physical crimes by definition. As an example, the crime of releasing hazardous substances in the United States is defined as a release made "into or upon the navigable waters of the United States, adjoining shorelines, or into or upon the waters of the contiguous zone."[31]

2. Transnational-Physical Crime

By modern transportation, some previously local-physical crimes have transformed themselves into transnational-physical crimes. Development of technology has increased the ease and speed of trans-border movement and decreased the cost of that movement for the benefit of all, including criminals. Terrorists of one state now move across borders to receive military training, provide logistical support, and commit terrorist attacks in other states. Transnational criminal organizations have expanded in size and influence, searching for new markets to smuggle drugs, humans, and firearms across borders.

In addition, once the development of transportation technology

---

28. *Crimes Against Children*, INTERPOL, http://www.interpol.int/Crime-areas/Crimes-against-children/Crimes-against-children [https://perma.cc/2MZ7-A82P].

29. *The Dru Sjodin National Sex Offender Public Website*, U.S. DEPT. OF JUSTICE, https://www.nsopw.gov/en-us/Education/FactsStatistics?AspxAutoDetectCookieSupport=1 [https://perma.cc/3VQT-4NDE] ("An estimated 60% of perpetrators of sexual abuse are known to the child but are not family members, e.g., family friends, babysitters, child care providers, neighbors. About 30% of perpetrators of child sexual abuse are family members.").

30. Thomas L. Hafemeister, *Financial Abuse of the Elderly in Domestic Setting*, *in* ELDER MISTREATMENT: ABUSE, NEGLECT, AND EXPLOITATION IN AN AGING AMERICA 382, 384 (Richard J. Bonnie & Robert B. Wallace eds., Nat'l Academies Press 2003) https://www.ncbi.nlm.nih.gov/books/NBK98802/pdf/Bookshelf_NBK98802.pdf [https://perma.cc/Y9GC-RYYK].

31. 42 U.S.C. § 9603(b)(1) (1996).

further lowers the cost of criminals crossing borders over the breakeven point, crimes which currently exist as local-physical crimes could evolve into transnational-physical crimes. For instance, regarding the child abuse example mentioned above, a child abuser might displace the crime to foreign states where law is enforced poorly against child abuse.

With globalization and digitalization, these transnational-physical crimes increasingly accompany the modus operandi of global-digital crime, which does not require physically crossing borders. Terrorists or organized criminals communicate with members in foreign states through emails or phones to plan and coordinate operations. Although these acts may constitute an inchoate crime, which could be categorized as a global-digital crime, this Article clarifies that the distinction between a local-physical crime and a global-digital crime would only consider the main modus operandi of the complete crime to determine its classification within this taxonomy.

3. Global-Digital Crime

In the global-digital era, the exponential development of telecommunication technologies has increasingly globalized and digitalized crimes. This digitalization has globalized crimes and the harm they cause by minimizing or removing the cost constraints incurred in physically moving across borders.

By adopting new digitalized tactics in carrying out all or main parts of criminal acts, former local-physical and transnational crimes are now committed globally without physically crossing borders. For example, though mostly a local-physical crime, child sexual abuse could be committed without physical contact by an individual on the other side of the world through the Internet.[32] Moreover, once an individual has Internet access, regardless of location, they can easily sell illegal drugs through the "deep [w]eb."[33] Likewise, terrorist organizations are able to finance their operations abroad by layering their transactions to hide the ultimate destination through financial institutions in multiple jurisdictions.[34] Corrupt officers use shell companies abroad to launder

32. *See* Sonia Livingstone & Leslie Haddon, *EU Kids Online: Final Report*, at 10 (2009), http://www.lse.ac.uk/media@lse/research/EUKidsOnline/EU%20Kids%20I%20(2006-9)/EU%20Kids%20Online%20I%20Reports/EUKidsOnlineFinalReport.pdf [https://perma.cc/2ARC-KPS2].

33. Steven Nelson, *Buying Drugs Online Remains Easy, 2 Years After FBI Killed Silk Road*, U.S. NEWS (Oct. 2, 2015), http://www.usnews.com/news/articles/2015/10/02/buying-drugs-online-remains-easy-2-years-after-fbi-killed-silk-road [https://perma.cc/4BHX-TTEH].

34. Press Release, *Remarks of Under Secretary for Terrorism and Financial Intelligence David Cohen Before the Center for a New American Security on "Confronting New Threats in Terrorist Financing"*, U.S. DEPT. OF TREASURY (Mar. 4, 2014), https://www.treasury.gov/press-center/press-releases/Pages/jl2308.aspx [https://perma.cc/92JN-25JH].

illicit funds obtained from foreign or domestic companies through the international financial system.[35]

Additionally, formerly non-existent digitalized crimes, such as cyber child pornography, cyber security incidents, and data breaches have emerged. These new crimes rely on the ability of data to move freely through cable networks regardless of physical, territorial boundaries.[36] Two recent high-profile examples may help illustrate the types of crime that fall into this group. First, it was alleged that North Korea, by deploying destructive malware, was able to destroy Sony's systems and steal sensitive personal and commercial data without entering U.S. territory.[37] Second, seven Iranians were indicted for their Digital Denial of Service ("DDoS") attacks: attacks using a group of devices located across the Internet and "remotely controlled by hackers without the knowledge of the rightful owner,"[38] against nearly fifty institutions in the U.S. financial sector, which resulted in the loss of tens of millions of dollars.[39] Clearly, global-digital crime is a type of crime that is growing steadily more significant for law enforcement officials and the victims of those crimes. The following section seeks to address how we might measure the efficiency by which law enforcement officials combat these three categories of crimes.

B. Methods of Analysis: Efficiency

This research engages in efficiency analysis by focusing on the characteristics of a "duty to report crime" as an administrative law. However, the moral culpability test, which was discussed in earlier criminal-law-focused research, is also helpful. Therefore, this Article utilizes the analytical framework and principles derived from the moral culpability test.

In measuring output, the crime deterrence, which I explained in my

---

35. Scott Shane, *Panama Papers Reveal Wide Use of Shell Companies by African Officials*, N.Y. TIMES (July 25, 2016), http://www.nytimes.com/2016/07/25/world/americas/panama-papers-reveal-wide-use-of-shell-companies-by-african-officials.html?_r=0 [https://perma.cc/C9LD-ZMPA].

36. Dan Robel, *International Cybercrime Treaty: Looking Beyond Ratification,* at 25 (Aug. 15,2006), https://www.sans.org/reading-room/whitepapers/incident/international-cybercrime-treaty-ratification-1756 [https://perma.cc/UX9U-NDDK] ("As mentioned earlier, a person behind a computer can just as easily connect to a computer in another country across the ocean as a computer within the same general region.").

37. Press Release, Update on Sony Investigation, FBI (Dec. 19, 2014), https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation [https://perma.cc/4ADS-YAV8] (last visited Nov. 30, 2016).

38. Benoit Dupont, Hacking the Panopticon: Distributed Online Surveillance and Resistance, *in* SURVEILLANCE AND GOVERNANCE: CRIME CONTROL AND BEYOND 257, 268 (Eds. Mathieu Deflem & Jeffrey T. Ulmer, 2008).

39. Iranians Charged with Hacking U.S. Financial Sector, FBI (Mar. 24, 2016), https://www.fbi.gov/news/stories/2016/march/iranians-charged-with-hacking-us-financial-sector [https://perma.cc/E7KU-XLYY].

previous Article as a moral culpability factor of good produced by reporting,[40] is also assessed here by a different metric. This analysis is carried out by types of crime, based on the taxonomy set out in Section A above, to explore the disparity in the output of a "duty to report crime" caused by the "global" administrative regulation. To evaluate input, a principle (i.e. the provision of governmental crime information to private reporters) derived from the moral culpability test is studied as it significantly affects the cost for the choke point private actors. This piece further describes more details of the rationales.

This Article advocates for the efficiency test, recognizing that there are generally four criteria employed by the state, prospectively or retrospectively—effectiveness, cost-effectiveness, efficiency, and equity—in evaluating an administrative regulation.[41] Among these, cost-effectiveness and efficiency are widely accepted tools.[42] While cost-effectiveness aims to find the lowest-cost policy in achieving the same output, efficiency aims to observe the regulation with the minimum possible inputs and maximum possible outputs.[43] Since an output of the "duty to report crime" regulations—the deterrence of crime—cannot be assumed to be same as that required in the cost-effectiveness analysis, this Article employs the efficiency analysis.

This Article takes a qualitative approach in measuring efficiency. Generally, the efficiency of a regulation is evaluated in a quantitative way by comparing the monetary value of the output with the input and calculating the internal rate of return that equalizes the present monetary value of the output and input.[44] This quantitative analysis needs to focus on a specific law to measure the output and input. However, the purpose of this Part is to provide justification for the global regulations of "duty to report crime." Thus, the important task of quantitative efficiency analysis is left to future scholarship.

C. Global Regulations Effectuating the Domestic Regulations of a "Duty to Report Crime"

This Part considers whether the domestic regulations of a "duty to report crime" can maximize deterrence without any support from

---

40. Kang, *supra* note 1, at 377.

41.Cary Coglianese, *Measuring Regulatory Performance, in* THE ORGANIZATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT 18 (Aug. 2012), https://www.oecd.org/gov/regulatory-policy/1_coglianese%20web.pdf [https://perma.cc/ZP9Z-HEU5].

42. *Id.*

43. *Sourcebook for Evaluating Global and Regional Partnership Program*, WORLD BANK 65 (2007), http://siteresources.worldbank.org/EXTGLOREGPARPROG/Resources/grpp_sourcebook_chap11.pdf [https://perma.cc/PZ2J-2VUE].

44. *Id.*

international institutions or norms.

1. Crime Deterrence as a Policy Output

Crime deterrence as a policy output of an administrative "duty to report crime" is the same concept of crime deterrence under criminal law; although deterring bad acts is also part of the purpose of administrative law.

The only distinction between those two is the independent variable in the metric of crime deterrence. While criminal law effectuates crime deterrence with a strong punishment, the administrative regulatory "duty to report crime" accomplishes crime deterrence by raising the probability of punishment. Indeed, the administrative "duty to report crime" deters crimes with a higher crime detection rate (i.e. an increased chance of getting caught), which is regarded by many scholars as a crucial factor in deterring crime, sometimes even more than a stronger punishment.[45]

This crime deterrence can be subdivided into specific deterrence and general deterrence.[46] Specific deterrence is deterrence of "the individual criminal offender from committing that crime again in the future," while general deterrence is deterrence of the public other than the criminal offender from committing a crime.[47]

This paper considers both specific and general deterrence without distinction in assessing whether the output, a higher probability of punishment, will discourage not only the general public but also the individual offender. Instead, the probability of punishment will encompass general deterrence as probability of detection and specific deterrence as probability of arrest.[48]

This non-distinction contrasts with the distinction between specific and general deterrence made in my previous Article. The rationale behind this is to point out the different approaches adopted in justifying the "duty to report crime" law under administrative law in this Article and under criminal law in the previous one.

Administrative law aims to focus on "handing out benefits to large

45. Jennifer Arlen & Reinier Kraakman, *Controlling Corporate Misconduct: An Analysis of Corporate Liability Regimes*, 72 N.Y.U. L. REV. 687, 779 n. 22 (1997) ("[I]ndividuals . . . are more deterred by a high probability of a relatively low sanction than a low probability of a very high sanction.") (citing JAMES Q. WILSON & RICHARD J. HERRNSTEIN, CRIME & HUMAN NATURE 397–401 (1985)).

46. Jonathan Odo et al., *Deterrence Theory*, *in* ENCYCLOPEDIA OF PRISONS & CORRECTIONAL FACILITIES 233, 234 (Bosworth ed., 2005).

47. *Id.*

48. Arrest achieves specific deterrence. *See generally* George S. Bridges & James A. Stone, *Effects of Criminal Punishment on Perceived Threat of Punishment—Toward an Understanding of Specific Deterrence*, 23 J. OF RES. IN CRIM. & DELINQ. 207 (1986); FRANKLIN E. ZIMRING & GORDON J. HAWKINS, DETERRENCE: THE LEGAL THREAT IN CRIME CONTROL (1973).

numbers of recipients," as appropriately illustrated by Ronald A. Cass.[49] Accordingly, an administrative law could be justified when it achieves the optimal benefit from the perspective of the general public. In this sense, the distinction between specific and general deterrence is meaningless, as both are beneficial to the public.

By contrast, criminal law is oriented towards focusing "on specific conduct so outside the realm of the acceptable as to be criminal."[50] This specific criminal conduct is conceptualized in two ways, moralist and instrumentalist, which affect the metric of deterrence.[51] Instrumentalists view criminal law as "an efficient means to whatever goals the theory posits" and accept a similar metric of crime deterrence for administrative law by considering both specific and general deterrence as goals of criminal law.[52] On the contrary, moralists emphasize traditional culpability limitation from the perspective of an individual criminal offender.[53] Accordingly, moralists do not consider after effects, including crime deterrence, attained by using criminal punishment as a tool.

The previous piece adopts this moralist view to control over-criminalization, which is a by-product of the instrumentalist view.[54] In justifying the criminalization of a failure to report crime, it considers specific deterrence, not as an aim to achieve, but as a factor—the good (or reduced harm) caused by reporting—affecting one's immorality of non-reporting.[55] On the contrary, general deterrence was not considered, as it fails to satisfy causation: the good of general deterrence is too distant from the individual's act of reporting for it to be regarded as a cause of one's moral decision to report.[56]

2. Crime Deterrence in Terms of the Taxonomy of Crime

The expected value of crime deterrence of domestic "duty to report crime" regulations could vary without corresponding global regulations,

---

49. Ronald A. Cass, *Overcriminalization: Administrative Regulation, Prosecutorial Discretion, and the Rule of Law*, 15 ENGAGE NO. 2 (December 16, 2014), http://ssrn.com/abstract=2520533 [https://perma.cc/T67A-27SU].

50. *Id.*

51. *Theories of Criminal Law*, STANFORD ENCYCLOPEDIA OF PHILOSOPHY (May 14, 2013), http://plato.stanford.edu/entries/criminal-law/ [https://perma.cc/P8DL-46PS].

52. *Id.*

53. *Id.*

54. Kang, *supra* note 1, at 362.

55. *Id.* at 377 ("Based on crime reporting, state authorities detect the crime reported and deter the offender from materializing on-going or future harm through retribution or rehabilitation. In addition, using the reported information shared through state authorities, other private entities could detect and deter covert on-going or possible future crimes. All of these will lead to higher detection rates, resulting in general deterrence of crime. The overall quantity of good produced depends on the characteristics of crime: its type, magnitude, extensiveness, and continuity or repeatability of harm.").

56. *Id.* ("The harm mitigated by general deterrence is too distant from the act of reporting to qualify as the harm caused by non-reporting.").

depending on the types—local-physical, transnational-physical, or global-digital—of crimes. This Section discusses crime deterrence specifically in terms of each of these three types of crime.

i. Local-Physical Crime

Domestic regulations that establish a "duty to report" local-physical crimes can maximize crime deterrence effect, without coordination at the international level, by incorporating the increased detection rate to the furthest extent.

In relation to a probability of crime detection, domestic regulation of a "duty to report crime" would effectively deter potential offenders from committing the local-physical crime, as it is neither easy nor feasible for the crime to be displaced to foreign jurisdictions where such duties are absent. Criminal acts and harm caused by the local-physical crime tend to stay in the local jurisdiction of said domestic regulation and will be witnessed and reported by the required domestic choke point private actors. Simply put, awareness of the higher risk of getting caught will deter the potential offender from committing the crime.

For instance, crimes involving the sexual abuse of children are usually prosecuted locally; it would be difficult to remove them to foreign jurisdictions with lower detection rates (i.e. jurisdictions without a duty to report). Under U.S. federal law, school teachers, physicians, psychiatrists, and many other professionals are required to report suspected child abuse to the designated national authorities as soon as possible.[57] Although the designated professions and the definition of child abuse can vary by state, most states in the United States (forty-eight) have imposed a duty to report child abuse on certain professions.[58] Two other states require all persons to report child abuse.[59] Thus, there will generally be a higher detection rate of child abuse in the United States compared to other jurisdictions that do not have such a duty. Practically, it would be difficult for a parent in the United States who would commit child abuse, which is a local-physical crime, to evade higher domestic detection by moving to a foreign state without a duty to report child abuse or sending his or her child to a school or to a physician in the foreign state.

In addition, domestic regulations of the duty to report local-physical crimes fulfill their expected crime deterrence role because the effect of an increased crime detection rate, led by crime reporting, is less likely to be

57. 34 U.S.C. § 20341 (2017).

58. *See generally Mandatory Reporters of Child Abuse and Neglect*, CHILDREN'S BUREAU OF U.S. DEPT. OF HEALTH & HUMAN SERVICES, at 2 (2016), https://www.childwelfare.gov/pubPDFs/manda.pdf [https://perma.cc/BZ6Q-66F3].

59. *Id.*

diminished by the barriers of sovereignty. Reports of local-physical crime are made to the state authorities who have jurisdiction over the reported crime. The information and evidence about the crime and the harm caused by the crime remain within its jurisdiction. The state authorities have legal authority to access the necessary information and evidence located in their jurisdiction and to take necessary measures to minimize or eliminate the imminent harm.

For example, the harm caused by the crime of releasing hazardous substances is local to the navigable waters of the United States, which is the statutory subject of protection. To prevent the expansion of the harm caused by the toxic substance and to incapacitate and deter the offender, the U.S. authorities, without any permission or assistance from foreign states, can investigate and take necessary measures.

The foregoing analysis makes it clear that domestic regulations that create a duty to report local-physical crimes can attain their maximum output without such a duty being embraced at the global level. This may explain the absence of current international and regional legal instruments that require choke point private actors to report local-physical crimes.

At the international level, the United Nations adopted the Convention on the Rights of the Child in 1989 ("CRC") to provide special safeguards and care needed for the child by reason of his or her physical and mental immaturity.[60] Concerned with the increasing risk of sexual exploitation of children, in 2000 the United Nations subsequently drafted the Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography ("U.N. Optional Protocol").[61] However, neither the CRC nor the Optional Protocol mandates that state parties must adopt a regulation on the duty to report child abuse.[62]

At the regional level, in 2007, the Council of Europe adopted the Convention on the Protection of Children Against Sexual Exploitation and Sexual Abuse ("CoE Convention on the Protection of Children").[63] Although Article 12 of this Convention requires member states to encourage voluntary reporting of suspicious sexual exploitation or sexual abuse by ensuring exemption of liability from possible breach of confidentiality, it does not require any mandatory reporting.[64]

---

60. The Convention on the Rights of the Child, Pmbl. Nov. 20, 1989, 28 ILM 1456 (1989).

61. G.A. Res. 54/263, annex II, Optional Protocol to the Convention on the Rights of the Child on the Sale of Children, Child Prostitution and Child Pornography, U.N. Doc. A/54/49 (Jan. 18, 2002).

62. *Id.* art. 9. ("States Parties shall take *appropriate measures* aimed at effectively prohibiting the production and dissemination of material advertising the offences described in the present Protocol.") (emphasis added).

63. Council of Europe, Convention on the Protection of Children against Sexual Exploitation and Sexual Abuse, art 12(2), CETS No. 201 (2007).

64. *Id.* art. 12(1)–(2).

Although international laws on child abuse do not currently provide for mandatory reporting, these policies may not continue indefinitely. The CoE Convention on the Protection of Children identifies several choke point private actors—the information and communication technology sectors, the tourism and travel industry, and the banking and finance sectors—which are crucial for preventing sexual exploitation and the abuse of children.[65] As the modus operandi of child abuse increasingly involves advanced means of transportation and telecommunication technologies, a duty to report child abuse needs to be imposed at the global level on the identified choke point private actors.

ii. Transnational-Physical Crime

To achieve the expected crime deterrence outcome, regulation of the duty to report transnational-physical crime and enhanced cooperation between states should be embraced by international law. Unlike a local-physical crime, a transnational-physical crime is easily displaced to a foreign state without a "duty to report crime" to evade the higher domestic detection rate, thus lowering the probability of crime detection. If the cost of movement decreases further, it is plausible that a parent living in the United States might simply take his or her abused child to a physician in a foreign state where physicians are under no obligation to report child abuse. Even the lowered detection rate caused by crime displacement might not be fully transformed into an arrest due to barriers of sovereignty. The arrest will be conditioned on effective cooperation with the foreign states involved.

In terms of the modus operandi of drug trafficking, which mainly involves physically crossing borders, the UNNDPS requires "manufacturers, importers, exporters, wholesalers and retailers [to] inform the competent authorities of suspicious orders and transactions,"[66] and "a commercial carrier operating within the territory of the Party . . . [to report] to the appropriate authorities at the earliest opportunity all suspicious circumstances."[67] In order to transform detected crimes to arrests by strengthening cooperation between states, the UNNDPS calls for efficient use of INTERPOL.[68] The Convention also includes the basis of traditional cooperation: confiscation,[69] extradition,[70] mutual legal assistance,[71] and transfer of proceedings.[72] It further requires member

65. *Id.* art. 9(2).
66. UNNDPS, *supra* note 18, art. 12(9)(a).
67. *Id.* art 15(2)(b)(iii).
68. *Id.* art. 1.
69. *Id.* art. 5.
70. *Id.* art. 6.
71. *Id.* art. 7.

states to adopt other forms of cooperation to enhance the effectiveness of investigation by:

> Establish[ing] and maintain[ing] channels of communication between their competent agencies and services to facilitate the secure and rapid exchange of information" and "[c]o-operat[ing] with one another in conducting enquiries . . . concerning: (i) The identity, whereabouts and activities of persons suspected of being involved . . . ; (ii) The movement of proceeds or property derived from the commission of such offences; (iii) The movement of narcotic drugs.[73]

Despite these provisions concerning drug trafficking, there is a lack of global regulations requiring a duty to report other transnational-physical crimes that result in similar, or even greater, harm. For instance, unlike the private sector actors who are exploited by drug traffickers and who are required to report suspicious transactions, the private sector actors who are abused or sometimes targeted by terrorist attacks (other than financial institutions abused for the financing of terrorism, which will be dealt with as a global-digital crime)[74] are not under an obligation to report suspicious activities. None of the nineteen international conventions adopted to suppress different types of terrorism require such a duty to report suspicions of terrorist attacks.[75] Reverting to the hypothetical in the introduction, the airline would not have to report any suspicion of terrorism even if it were furnished with proper crime information through the SLTD database.

Instead, even in the absence of global regulations creating a "duty to report crime," transnational-physical crimes are exposed to higher detection by public authorities at the border. This somewhat complements lower detection by the private sector than local-physical crimes. Because transnational-physical crimes must physically cross the border, the criminals will go through inspections by border control authorities. As in the hypothetical example where the immigration officers could disrupt the terrorists' plot thanks to a positive match with INTERPOL's SLTD database, frontline public authorities at the border, supported by appropriate information-sharing and cooperation between states, add risk of detection to transnational-physical crimes.

iii. Global-Digital Crime

Regarding global-digital crimes, the domestic "duty to report crime" regulations, by themselves, without close coordination at the global level, would fail to maximize crime deterrence due to the same rationale—a

72. UNNDPS, *supra* note 18, art. 8.
73. *Id.* art. 9(1)(b).
74. *See infra* Part II.C.2.c.
75. *See, e.g.*, UNNDPS, *supra* note 18.

lower probability of crime detection caused by crime displacement and a lower probability of arrest prompted by barriers of sovereignty—which will mean they fail to deter transnational-physical crime.[76] Criminals in this global-digital era easily "leverage technology to conduct operations at a greater distance . . . which provide both physical and legal protection for offenders . . . while complicating governmental efforts to detect, investigate and disrupt transnational crimes and illicit activities."[77]

For instance, under 31 U.S.C. § 5318, financial institutions in the United States are required to report suspicious transactions[78] and to practice what is referred to as "Enhanced Due Diligence" for certain risky transactions,[79] including transactions involving foreign "Politically Exposed Persons" ("PEPs"). To avoid the high risk of detection in using U.S. financial institutions, corrupt foreign officers may open an account in the name of a shell company with a financial institution in a third jurisdiction that has no, or a less strict, "duty to report crime" provision. Bribers in the United States will use such financial institutions to launder illicit funds to be transferred to the corrupted officer, thereby easily lowering the risk of detection. Knowing this, potential offenders would not be deterred from committing global-digital crime.

In addition, the barriers of sovereignty, exemplified by the many provisos mentioned below, hinder the crime detection-to-arrest process. Even when a financial institution in a third jurisdiction can detect the suspicious transaction of unlawful funds, it will report to its own state agency. The foreign state authorities with the reported information will communicate the information, if they wish, to U.S. authorities who have jurisdiction over the corruption following their own domestic mutual legal assistance law or treaties between the two states. While proceeding with the investigation, foreign authorities may or may not assist in obtaining evidence and information located in their jurisdiction, as requested by U.S. authorities. All these processes provide legal and physical protection to the criminal and lower the possibility of apprehension of suspects.

Enactment of a global regulation establishing a "duty to report crime" is particularly essential for the deterrence of global-digital crimes, more so than for transnational-physical crimes. Although deterrence of transnational-physical crimes diminishes due to crime displacement and sovereignty barriers, this lowered deterrence is somewhat compensated for

---

76. This problem of crime displacement is properly described as a "third-country problem" in relation to tax evasion, where money freely trespasses national boundaries through international financial networks. *See* Michael Keen & Jenny E. Ligthart, *Information Sharing and International Taxation*, 13 INT. TAX & PUB. FIN. 81, 89–91 (2006).

77. Joseph Schafer, *International Police Cooperation*, *in* CRIMINOLOGY (2014).

78. 31 U.S.C. § 5318(g)(1) (2014).

79. *Id.* § 5318(i)(2)(B) (2014).

by the additional public detection by frontline law enforcement officers at the border. However, global-digital crimes have no such borders to physically cross, thus no frontline law enforcement authorities exist, other than the choke point private actors providing the digitalized services that the criminals exploit. For example, unlike the attempted terrorist attack alluded to in our hypothetical, which is a transnational-physical crime detected by the frontline officers at the border, the financing of terrorism is carried out through the global web of digitalized financial transactions—it has no equivalent border controlled by frontline officers. Thus, the role of choke point private actors, the financial institutions in the example, is extremely important in deterring crimes in this global-digital era.

In sum, without global regulation requiring choke point private actors to report global-digital crimes, even states that have enacted domestic regulations creating a duty to report global-digital crime ultimately will suffer from a lower crime deterrence mechanism. Thus, international society has adopted regulations on "duty to report crimes" with global-digitalized modus operandi, most of which involve abusing Internet or financial services for criminal purposes.

3. Lack of Global Regulation of a "Duty to Report Crime" in the Global-Digital Era

With regards to crimes that exploit global-digitalized financial services, most of which are financing or laundering the proceeds of crime, the UNICSFT requires that:

> [F]inancial institutions and other professions involved in financial transactions [utilize] the most efficient measures available for the identification of their usual or occasional customers, as well as customers in whose interest accounts are opened, and to pay special attention to unusual or suspicious transactions and report transactions suspected of stemming from a criminal activity.[80]

In addition, the UNTOC[81] and UNCAC[82] also impose similar duties on financial institutions.

In contrast, regarding crimes that exploit global-digitalized Internet services, international society has been slow to reach a consensus, while domestic laws have established a duty to report such crimes.[83] However, as Professor Harold Hongju Koh states, "[c]yberspace is not a 'law-free'

80. UNICSFT, *supra* note 18, art. 18(1)(b).
81. *Id.* art 7(1)(a).
82. *Id.* art. 14(1)(a).
83. For instance, the United States adopted a duty to report cyber incidents by Department of Defense contractors. *See* 32 C.F.R. § 236 (2016). In addition, a duty to report security breaches has been imposed at the federal level on the health insurance industry and at the local level on general businesses. *See, e.g.*, 42 U.S.C. § 1320d-5 (2012); N.C. GEN. STAT. ANN. § 75-65 (West 2009).

zone where anyone can conduct hostile activities without rules or restraint," but instead international society needs to "articulate and build consensus around how [the existing rule] applies and reassess from there whether and what additional understandings are needed."[84]

Only regional agreements, which regulate cyberspace, include a duty to report cyber security incidents and data breaches. While the Convention on Cybercrime adopted by the Council of Europe in 2001 focuses on criminal policy coordination for cybercrime investigation,[85] the following two EU Directives aim to manage security risks of network[86] and personal data[87] by improving the preparedness of member states, including mandatory reporting by certain private service providers of cyber incidents or data breaches to the national competent authorities. First, the E-privacy Directive was adopted and entered into in 2002, and amended in 2006 and 2009.[88] The amended E-privacy Directive requires "the provider of publicly available electronic communications services [to], without undue delay, notify the personal data breach to the competent national authority."[89] Second, the NIS Directive was adopted and entered into in 2016.[90] It requires "Member States [to] ensure that operators of essential services notify, without undue delay, the competent authority or the CSIRT of incidents having a significant impact on the continuity of the essential services they provide."[91]

Regarding online child pornography, legal instruments at both the international and regional level fail to impose a mandatory reporting duty on the private sector, while acknowledging the role of the Internet and developing technologies in increasing accessibility to child pornography. The UN Optional Protocol emphasizes in its preamble, "the importance of closer cooperation and partnership between Governments and the Internet Industry."[92] However, other than in the preamble, the Optional Protocol does not mention the role of the private sector nor does it provide any specific measures, including mandatory reporting of child pornography, to be taken by the state parties.[93]

At the regional level, the CoE Convention on the Protection of

84. Harold Hongju Koh, *International Law in Cyberspace*, 54 HARVARD INT'L L.J. ONLINE 1, 3 (2012).

85. Convention on Cybercrime, 23.XI.2001, ETS 185, Pmbl. ("Convinced of the need to pursue, as a matter of priority, a common criminal policy aimed at the protection of society against cybercrime, inter alia, by adopting appropriate legislation and fostering international co-operation.").

86. NIS Directive, *supra* note 20.

87. E-Privacy Directive, *supra* note 19.

88. *Id.*

89. *Id.* art. 4.

90. *See generally* NIS Directive, *supra* note 20.

91. *Id.* art. 14.

92. Optional Protocol, *supra* note 61, at pmbl.

93. *Id.* art. 9.

Children, in tackling the issue of child pornography as one of the means for the sexual exploitation of children,[94] recognizes information and communication technologies as an important contributing factor to the rapid growth in sexual exploitation and abuse of children.[95] In a number of provisions, the CoE Convention on the Protection of Children emphasizes and encourages the participation of the private sector[96] and cooperation between competent state authorities and the private sector.[97] However, the Convention fails to mandate reporting.[98]

Additionally, in 2011, the EU adopted the Directive on Combating Sexual Abuse and Sexual Exploitation of Children and Child Pornography ("Directive on Sexual Abuse of Children"). The Directive updates the CoE Convention on the Protection of Children but still does not impose a mandatory duty to report. In relation to reporting suspected child pornography, it simply requires member states to "take appropriate action for setting up information services to provide information on how to recognize the signs of sexual abuse and sexual exploitation,"[99] and to promote a hotline reporting system.[100]

Overall, the necessity and importance of a global obligation and a mandatory "duty to report crime" have been recognized by the international society, but such regulation is still lacking for many global-digital crimes. Thus, Section D argues that, for the currently existing and forthcoming global regulations concerning a "duty to report crime" to be more efficient, it is timely to perceive a vital component of the regulation.

D. Global Regulation of a (Bottom-Up) "Duty to Report Crime" Incorporating (Top-Down) Vertical Cooperation

1. Top-Down Vertical Cooperation and Policy Input

Global regulation of a "duty to report crime" to deter global-digital

94. Council of Europe, *supra* note 63, art. 3(b) ("'[S]exual exploitation and sexual abuse of children' shall include the behaviour as referred to in Articles 18 to 23 of this Convention."); *id.* art. 20 (describing offences concerning child pornography).

95. *Id.* at pmbl. ("Observing that the sexual exploitation and sexual abuse of children have grown to worrying proportions at both national and international level, in particular as regards the increased use by both children and perpetrators of information and communication technologies (ICTs), and that preventing and combating such sexual exploitation and sexual abuse of children require international co-operation.").

96. *Id.* art. 9(2), art. 12.

97. *Id.* art. 10(3) ("Each Party shall encourage co-operation between the competent state authorities, civil society and the private sector, in order to better prevent and combat sexual exploitation and sexual abuse of children.").

98. *Id.* art. 12(2).

99. Directive 2011/93, of the European Parliament and of the Council of 13 December 2011 on Combating the Sexual Abuse and Sexual Exploitation of Children and Child Pornography, and Replacing Council Framework Decision 2004/68/JHA, ¶ 45, 2011 O.J. (L 335)1 (EU).

100. *Id.* ¶ 35.

crime should incorporate the provision of governmental[101] crime information to choke point private actors (i.e. top-down cooperation). Top-down cooperation is crucial to minimizing the policy input, namely the cost.

Above all, top-down cooperation reduces the cost of enforcement born by the government while securing higher compliance. Top-down cooperation was originally suggested in the previous Article in relation to a required principle to justify criminalization of a failure to report crime.[102] The argument is that criminal penalties should be employed only for the most morally culpable behaviors; the principles suggested in the previous Article, including top-down cooperation, create the contexts whereby the choke point private actors are the most strongly morally obliged to report crime.[103] When the law is enforcing widely-accepted moral norms, the cost of enforcement to make the obligors comply with the law is reduced.[104]

The unnecessary burden on the private sector[105] to comply with the duty to report will be eliminated by top-down cooperation, since it will "lower the level of harm to a reporter by cutting the information collecting cost and harm to the individual being reported by decreasing the possibility of erroneous reporting."[106] The previous research illustrated this with an example concerning PEPs, which referred to the information possessed by the government but kept from financial institutions in need of the information to comply with their duty to report.[107] That Article demonstrated the lack of sharing PEPs' information caused "unnecessary[ily] huge costs and greater dissipation of resources for overall [domestic] society due to a duplication of cost and efforts."[108] Considering that this Article deals with global regulation of a "duty to report crime," the unnecessary burden on the global private sector that could be eliminated by sharing governmental information with choke

101. The governmental crime information is possessed by the government and includes both the information the government itself collects and stores in its database and the information reported by choke point private actors, or the public to the government.

102. Kang, *supra* note 1, at 393.

103. *Id.* at 374–78.

104. *Id.* at 371–72 ("The importance of enforcement differs depending on the way the law affects behavior. For instance, to be an effective law, a prohibition on murder, which enforces a widely accepted moral code, does not require as much enforcement as a prohibition on smoking marijuana, which, depending on the individual, manipulates or expresses certain moral codes.") (citations omitted).

105. MARTÍN MOLINUEVO & SEBASTIÁN SÁEZ, REGULATORY ASSESSMENT TOOLKIT: A PRACTICAL METHODOLOGY FOR ASSESSING REGULATION ON TRADE AND INVESTMENTS IN SERVICES 21 (The World Bank 2014) ("Efficiency considerations can also play a role in regulation for noneconomic goals. An efficient regulation seeks to achieve public interest goals and avoid introducing unnecessary burdens in the market.").

106. Kang, *supra* note 1, at 392.

107. *Id.* at 394.

108. *Id.* at 395.

point private actors is enormous.

To secure efficiency by minimizing policy input, global regulation of a "duty to report crime" should employ this critical component of providing governmental information to choke point private actors (i.e. top-down cooperation). Further, because the government requires the choke point private actors to take a frontline law enforcement role (which is originally the responsibility of the government), there is a counter-duty on the government to minimize the burden of the choke point private actors in carrying out such a role.

The principle of sharing governmental crime information with choke point private actors should be respected regardless of the position of the reporter to the crime. Although this principle was discussed regarding a third-party reporter who has intrinsically limited information about the crime, even an offender reporter and a victim reporter, who tend to be in a better position regarding information about the crime, could also fail to recognize the crime committed.[109]

2. Lack of Top-Down Vertical Cooperation in Contemporary Global "Duty to Report Crime" Regulations

To deter some transnational-physical crimes and global-digital crimes, international and regional frameworks have been adopted that establish a "duty to report crime." However, no international or regional regulations that stipulate a "duty to report crime" (i.e. bottom-up cooperation) incorporate this vital component, namely, providing governmental information to choke point private actors (i.e. top-down cooperation) in their provisions, as illustrated below.

None of the international agreements discussed above (the UNNDPS, UNICSFT, UNTOC, nor the UNCAC) require governmental crime information to be provided to choke point private actors. With regards to the regulation of a "duty to report crime" at the regional level, the EU NIS Directive allows member states, after consulting the reporter, to inform the public about cyber incidents.[110] However, sharing crime information with the public, although helpful for choke point private actors as a source of

---

109. *See id.* at 378–79 ("A person with superior responsibility might fail to recognize the crime committed by its employee bribing foreign officials to increase sales, as the employee will try to hide his wrongdoings by breaching the internal compliance regulations of his employer. A victim could fail to recognize data breaches or cyber incidents, as hackers tend to hide their attacks on victim's system to maximize harm."); *see also* TERRENCE K. KELLY & JEFFREY HUNKER, *Cyber Policy: Institutional Struggle in a Transformed World*, *in* CYBERSECURITY: SHARED RISKS, SHARED RESPONSIBILITIES 3, 25 (Peter M. Shane & Jeffrey Hunker eds., 2013) ("The logic underlying public-private partnerships includes the government's assumption that infrastructure owners will 'do the right things' . . . . However, in the face of uncertain threats, there is no common understanding of what the right thing is.").

110. NIS Directive, *supra* note 20, art. 14(6).

crime information to be used, is different from sharing with choke point private actors, as will be illustrated in the later part of this paper.[111] The E-privacy Directive establishes no such measure to share governmental crime information with choke point private actors.

III. A LEGISLATIVE BLUEPRINT FOR THE GLOBAL REGULATION OF A "DUTY TO REPORT CRIME"

This Part answers how the legislative efforts at the international level should manage demanded mutual vertical cooperation, particularly with the current lack of top-down cooperation. Specifically, it considers how to channel the requisite domestic governmental crime information to foreign choke point private actors. Drafting a legislative blueprint is crucial for making proper modifications to existing global regulations of a "duty to report crime" and for enacting new regulations that are lacking in relation to several global-digital crimes.

This Part proposes an ideal regime, an international, instantaneous sharing regime, for top-down cooperation. However, there are three caveats for the ideal regime to be justified as feasible and legitimate: horizontal accountability; vertical accountability; and proportionality to privacy/reputational harm to the subject of the shared information.[112] Rationales that consider theories of international relations, global administrative law theory, and privacy rights are offered for each caveat. These rationales will be followed by the suggestion of a practical model to actualize the ideal regime based on the analysis of possibilities and limitations of contemporary architecture of international governmental crime information sharing with choke point private actors.

A. The Ideal Regime for Top-Down Vertical Cooperation: International, Instantaneous Sharing

In order to obtain optimal efficiency of "duty to report crime" laws in the modern era, the principle of providing governmental crime information to choke point private actors (i.e. top-down cooperation), derived from the analysis on domestic laws in the previous Article, should be extended to corresponding international laws. This means the global regulation of a "duty to report crime" should require states to provide their governmental information to their domestic choke point private actors; but it is not limited to that obligation. The proposal also includes an obligation that

111. *See infra* Part III.B.2.iii.

112. *See* Kang, *supra* note 9, at 19. ("[T]he global AML/PEP regulatory body, whether it is the UN or the FATF, should respect three essential values: accountability of States providing the list to foreign States/financial institutions, accountability to the listed domestic PEPs and protection of the PEPs' privacy.").

states should supply their governmental crime information to foreign choke point private actors. In other words, the ideal top-down cooperation should be international, not solely domestic.

Enactment of global regulations establishing a "duty to report crime" will fail to achieve optimal efficiency when the choke point private actors are not supplied with the required foreign crime information. Ensuring the absence of legal-loophole states across the globe should be supported by the absence of information-loophole choke point private actors across the globe. This is particularly crucial where the choke point private actors are in the frontline in relation to deterring crimes that are easily and instantaneously displaced from one jurisdiction to another: global-digital crimes.

A specific example helps illustrate the point. Even if financial institutions in all jurisdictions are required to report suspicious transactions related to corruption and are legally authorized to access the list of domestic PEPs possessed by their governments, the expected policy output (corruption detection) would impact only corrupt domestic officers using domestic financial institutions. Without access to the list of foreign PEPs possessed by foreign governments, the financial institutions could easily be abused by corrupt foreign officers. In other words, to evade the risk of higher detection, corrupt domestic officers need only utilize foreign financial institutions that lack information about their status as PEPs. Alternatively, when financial institutions are required to gather foreign PEP information on their own, the policy input of information gathering cost would be enormous.

Further, the ideal regime should not just be international, but also instantaneous. Domestic choke point private actors can access crime information possessed by foreign governments through various channels.[113] However, unless there is a robust instantaneous reach to the information, the policy output will be limited. Lengthy, complicated channels will provide criminals with opportunities to abuse information-loopholes until the choke point private actors are finally able to access the requisite information.

A few examples help illustrate the effects of non-instantaneous availability of information. The lapse of time provides criminals with opportunities to layer their illicit proceeds through multiple financial transactions, thus lowering the risk of crime detection.[114] The longer dwell time allows hackers to materialize and aggravate the harm of cyber incidents and data breaches, thus producing more victims, while

113. *See infra* Chart I.

114. *See* PETER REUTER & EDWIN M. TRUMAN, CHASING DIRTY MONEY: THE FIGHT AGAINST MONEY LAUNDERING 30 (Inst. for Int'l Econ. 2004).

eradicating evidence of the crime at the victim's network.[115] Child pornography will spread rapidly and widely over time throughout the Internet; this will have a devastating effect on the abused children and a corrosive effect on viewers.[116]

Lastly, to attain an instantaneous and international ideal regime, the communication channel between states and choke point private actors should be characterized by proactive information sharing rather than reactive information exchange.[117]

Under the information exchange, choke point private actors encounter obstructions to instantaneous access to foreign governmental crime information. To request information, choke point private actors should first investigate and verify the destination of the request, then wait for the response. Most importantly, reactive information exchange, based on the assumption of a "need to know" threshold before it is shared,[118] fails to assist choke point private actors to detect crimes where no suspicions have been raised to trigger a request for crime information. When they fail to recognize the hidden crime committed or when they wrongly believe that what they witness is not a crime, information exchange will be of no help.

In contrast, sharing information requires states, even without a request for information from choke point private actors, to proactively establish and continuously update databases that are promptly accessible by the authorized choke point private actors. This assists choke point private actors to detect and deter crime that is not initially recognized as crime. For example, for cyber criminals, who usually hide their intrusion into a victim's network for a long dwell time, shared information such as IP addresses or file names would allow the victim to locate the hidden attack, thus minimizing the harm. Furthermore, an ISP that encounters ambiguous child pornography could detect and confirm the crime utilizing the shared information of hash values or a list of URLs of child pornography.

---

115. ARBOR NETWORKS, *New Ponemon Institute Survey Revelations on Timing* (May 19, 2015), https://www.arbornetworks.com/new-ponemon-institute-survey-reveals-time-to-identify-advanced-threats-is-98-days-for-financial-services-firms-197-days-for-retail [https://perma.cc/NYD8-SS5Q].

116. *See generally* CENTER FOR PROBLEM-ORIENTED POLICING, *Effects of Child Pornography*, http://www.popcenter.org/problems/child_pornography/2 [https://perma.cc/572W-QMYB].

117. INTERPOL, *Effective Information Sharing Underpins Efforts Against Nuclear Terrorism—INTERPOL Chief* (April 1, 2016), http://www.interpol.int/News-and-media/News/2016/N2016-041/ [https://perma.cc/B4HR-H54M] ("Targeting criminals and terrorists, and curbing their potential to pursue their goal requires proactive, systematic sharing of and access to information as a key part of our collective security mandate.").

118. NAT'L COMM'N ON TERRORIST ATTACKS UPON THE U.S., *The 9/11 Commission Report*, at 417 (2004), https://9-11commission.gov/report/911Report.pdf [https://perma.cc/PWL4-R9XC] ("In the 9/11 story, for example, we sometimes see examples of information that could be accessed—like the undistributed NSA information that would have helped identify Nawaf al Hazmi in January 2000. But someone had to ask for it. In that case, no one did.").

Accordingly, to optimally achieve their purpose of crime deterrence, global regulations creating a "duty to report crime" should mandate states to take appropriate and effective measures to instantaneously share crime information with choke point private actors, including foreign ones. This ideal regime may not be possible, but it is helpful to think in these terms to understand what the goal should be. To actualize the ideal regime, the following Section suggests how global regulation of a "duty to report crime" should be shaped by studying the possibilities and limitations of the contemporary architecture of international top-down cooperation.

B. Possibilities and Limitations of the Contemporary Architecture of International Top-Down Vertical Cooperation

1. Contemporary Architecture of International Top-Down Vertical Cooperation

This part examines the contemporary architecture of international top-down cooperation. It draws a comprehensive map of current crime information flow[119] between various actors at the international level—public, private entity, government, and international organizations ("IOs")—which have not been fully explored in other academic works.

Post-9/11 scholarship has focused on information sharing to deter crime, particularly terrorist attacks, with most studies limiting themselves to the domestic level.[120] There have also been individual case studies of

---

119. This will only include systemized information sharing with certain sets of procedure with designated authority. Accordingly, random information sharing will not be studied. In addition, only proactive information sharing systems will be analyzed, as reactive information exchange does not satisfy the instantaneous sharing components of an ideal regime.

120. Scholars on domestic information sharing have studied cooperation between different domestic actors, emphasizing information sharing between federal agencies, particularly intelligence and law enforcement agencies. See Craig S. Lerner, The USA PATRIOT Act: Promoting the Cooperation of Foreign Intelligence Gathering and Law Enforcement, 11 GEO. MASON L. REV. 493, 524–26 (2003); RICHARD A. POSNER, PREVENTING SURPRISE ATTACKS: INTELLIGENCE REFORM IN THE WAKE OF 9/11 at 26 (2005); see generally Richard Henry Seamon & William Dylan Gardner, The PATRIOT Act and the Wall Between Foreign Intelligence and Law Enforcement, 28 HARV. J.L. & PUB. POL'Y 319 (2005); Nathan Sales, Share and Share Alike: Intelligence Agencies, Information Sharing, and National Security, 78 GEO. WASH. L. REV. 279 (2010); Nathan Sales, Mending Walls: Information Sharing After the USA PATRIOT Act, 88 TEX. L. REV. 1795 (2010); Danielle Keats Citron & Frank Pasquale, Network Accountability for the Domestic Intelligence Apparatus, 62 HASTINGS L.J. 1441. Also, information sharing between federal agencies and local enforcement authorities is another common field of study. See, e.g, DAVID L. CARTER, LAW ENFORCEMENT INTELLIGENCE: A GUIDE FOR STATE, LOCAL, AND TRIBAL LAW ENFORCEMENT AGENCIES (2004); Matthew C. Waxman, Police and National Security: American Local Law Enforcement and Counterterrorism After 9/11, 3 J. NAT'L SECURITY L. & POL'Y 377 (2009); Samuel J. Rascoff, The Law of Homegrown (Counter) Terrorism, 88 TEX. L. REV. 1715, 1726 (2010); Jason B. Jones, Note, The Necessity of Federal Intelligence Sharing with Sub-Federal Agencies, 16 TEX. REV. L. & POL. 175, 199 (2011); Lindsey Garber, Have We Learned A Lesson? The Boston Marathon Bombings and Information Sharing, 67 ADMIN. L. REV. 221 (2015). In addition, though mostly limited to certain national critical infrastructures or cyber aspects of terrorism, several researches have analyzed public-private information sharing. See, e.g., MARKLE FOUND., CREATING A TRUSTED INFORMATION NETWORK FOR HOMELAND SECURITY: SECOND REPORT OF THE MARKLE FOUNDATION TASK FORCE

international information sharing or exchange regimes in criminal matters, such as Europol,[121] INTERPOL,[122] or Mutual Legal Assistance Treaties.[123] Even research that compares different regimes of international crime information sharing tends to focus solely on state-to-state horizontal sharing.[124] This Article contributes to the scholarship by drawing together generalizations from across these studies to offer a coherent and comprehensive architecture for such transnational crime information-sharing regimes, as indicated in Chart I below and the explanatory notes that follow it.[125]

(2003); Kristen Elizabeth Uhl, The Freedom of Information Act Post-9/11: Balancing the Public's Right to Know, Critical Infrastructure Protection, and Homeland Security, 53 AM. U. L. REV. 261 (2003); D. Richard Rasmussen, Is International Travel Per Se Suspicion of Terrorism? The Dispute Between the United States and European Union over Passenger Name Record Data Transfers, 26 WIS. INT'L L.J. 551 (2008); Elaine M. Sedenberg & Deirdre K. Mulligan, Public Health as a Model for Cybersecurity Information Sharing, 30 BERKELEY TECH. L.J. 1687 (2015); John P. Carlin, Detect, Disrupt, Deter: A Whole-of-Government Approach to National Security Cyber Threats,7 HARV. NAT'L SEC. J. 391 (2016).

121. *See* Julia Ballaschk, *In the Unseen Realm: Transnational Intelligence Sharing in the European Union—Challenges to Fundamental Rights and Democratic Legitimacy*, 51 STAN. J. INT'L L. 19 (2015); Frank Cali, *Europol's Data Protection Mechanisms: What Do They Know and Whom Are They Telling?*, 10 TOURO INT'L L. REV. 189 (2000); Jacqueline Klosek, *The Development of International Police Cooperation Within the EU and Between the EU and Third Party States: A Discussion of the Legal Bases of Such Cooperation and the Problems and Promises Resulting Thereof*, 14 AM. U. INT'L L. REV. 599 (1999); Francis R. Monaco, Comment, *Europol: The Culmination of the European Union's International Police Cooperation Efforts*, 19 FORDHAM INT'L L.J. 247 (1995).

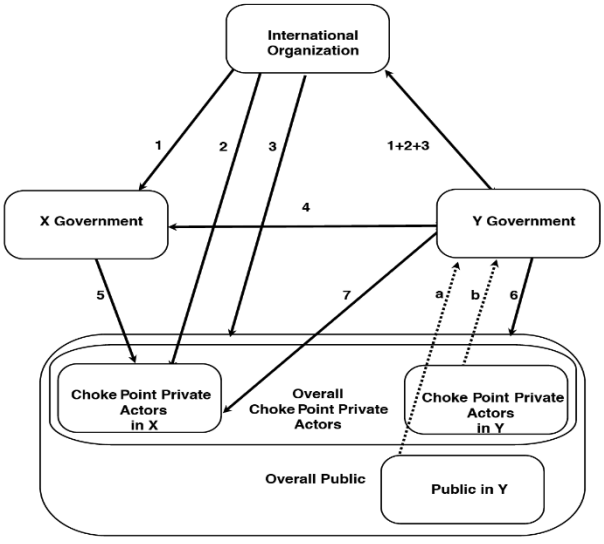
122. *See* Nina Marino & Reed Granthama, *Wanted by Interpol: Strategic Thinking About Red Notices, Diffusions, and Extradition*, 30 CRIM. JUST. 4 (2015); Mario Savino, *Global Administrative Law Meets 'Soft' Powers: The Uncomfortable Case of Interpol Red Notices*, 43 N.Y.U. J. INT'L L. & POL. 263 (2011); Peter M. Thomson, *Interpol's Transnational Policing by "Red Notice" and "Diffusions": Procedural Standards, Systemic Abuses, and Reforms Necessary to Assure Fairness and Integrity*, 16 ENGAGE: J. FEDERALIST SOC'Y PRAC. GROUPS 23 (2015); Corey Winer, *Smoke 'Em Out: U.S. Counterterrorist Mishaps Necessitating the Expansion of Interpol's Capabilities to Meet the New Terrorist Threat*, 33 SUFFOLK TRANSNAT'L L. REV. 145 (2010); Jacques Semmelman & Emily Spencer Munson, *Interpol Red Notices and Diffusions: Powerful—And Dangerous—Tools of Global Law Enforcement*, CHAMPION, May 2014, at 28.

123. *See* Robert Neale Lyman, *Compulsory Process in a Globalized Era: Defendant Access to Mutual Legal Assistance Treaties*, 47 VA. J. INT'L L. 261 (2006); L. Song Richardson, *Convicting the Innocent in Transnational Criminal Cases: A Comparative Institutional Analysis Approach to the Problem*, 26 BERKELEY J. INT'L L. 62 (2008); Thomas G. Snow, *The Investigation and Prosecution of White Collar Crime: International Challenges and the Legal Tools Available to Address Them*,11 WM. & MARY BILL RTS. J. 209 (2002).

124. *See* James B. Jacobs & Dimitra Blitsa, *Sharing Criminal Records: The United States, the European Union and Interpol Compared*, 30 LOY. L.A. INT'L & COMP. L. REV. 125 (2008).

125. Governmental crime information includes not only the information provided by its domestic public (flow "a" in Chart I) and choke point private actors (flow "b" in Chart I), but also the information collected by itself (e.g. criminal history records) and the results of any information analysis carried out by the government. Flow of crime information originated from choke point private actors and public are a crucial but partial portion of governmental crime information. Thus, the focus of this analysis is to show how governmental crime information can reach, either directly or indirectly through international organizations or foreign states, the foreign choke point private actors in need of such information to deter crime. Other possible crime information flows that have no or remote relationship with this purpose are not studied. This Article does not consider other possible information flows, apart from their feasibility and practicality as a systemic legal regime, originating from choke point private or public actors beyond flows "a" and "b" in Chart I (e.g. domestic choke point private actors to foreign governments or IOs or overall/foreign choke point private actors or overall public; domestic public to foreign governments or IOs or overall/foreign choke point private actors or overall public). This does not mean that these possible but unaddressed information flows are not necessary. As long as feasibility and practicality are satisfied, these flows should be

Chart I: Contemporary Architecture of International Top-Down Vertical Cooperation



Crime information flow paths[126]

The following is a description of each information source in Chart I and some examples of the potential sources of information[127] along each numbered flow path:

1. INTERPOL's International Child Sexual Exploitation image database;

encouraged, ideally along with the provider of governmental crime information, to support better instantaneous, international sharing of crime information. These flows would become more crucial when other sources of governmental crime information are absent. For instance, information sharing between choke point private actors in the United States is encouraged under Section 314(b) of the USA PATRIOT Act by providing safe harbor for voluntarily sharing information between financial institutions that may involve possible terrorist or money laundering activities. *See* FIN. CRIMES ENFORCEMENT NETWORK, *Section 314(b) Fact Sheet*, https://www.fincen.gov/sites/default/files/shared/314bfactsheet.pdf [https://perma.cc/3VK3-JEM6]. As the Financial Crimes Enforcement Network ("FinCEN") does not provide financial institutions the governmental information corresponding to the information they voluntarily share, this section of the USA PATRIOT Act should be strongly encouraged. Similarly, information sharing between choke point private actors at the international level should be encouraged. Finally, based on the Zero Day Initiative in the United States, information flow from public to choke point private actors is encouraged on a contractual basis. *See* Mohit Kumar, *New Internet Explorer Zero-Day Vulnerability Publicly Disclosed*, THE HACKER NEWS (May 21, 2014), http://thehackernews.com/2014/05/internet-explorer-zero-day.html [https://perma.cc/FX7Y-5Z53] ("Zero Day Initiative is a program for rewarding security researchers for responsibly disclosing vulnerabilities."). This initiative encourages the public, which does not have a duty to report crime, to do so anyway, thus increasing crime deterrence. *Id.*

126. The list of precedents for each flow of crime information is not exhaustive.

127. Other than the international sources, such as the U.N., EU, and INTERPOL, domestic sources given as examples in this Article solely focus on U.S. laws or policies.

DNA Gateway; Fingerprint database[128]

2. INTERPOL's I-Checkit program[129]
3. United Nations Security Council 1373 Sanction Committee's list of terror organizations and terrorists; INTERPOL's list of wanted persons (Red Notice) or persons presenting an imminent threat (Yellow Notice); Financial Action Task Force ("FATF") high-risk and non-cooperative jurisdictions list (formerly, NCCT List)[130]
4. Agreement between the Government of Canada and the Government of the United States of America for the Sharing of Visa and Immigration Information; The Nordic Mutual Assistance Convention on Mutual Administrative Assistance in Tax Matters ("The Nordic Mutual Assistance Convention"); Council Directive 2014/107/EU amending Directive 2011/16/EU on Administrative Cooperation in the Field of Taxation ("DAC2")[131]

---

128. IOs work as database centers and allow access only to authorized government authorities through their own platforms. For instance, INTERPOL, through its International Child Sexual Exploitation image database, DNA Gateway, Fingerprint database, SLTD, and others, collects information in criminal matters from each member state and provides access to the shared information to authorized state authorities of the member states. *See* INTERPOL, Databases, http://www.interpol.int/INTERPOL-expertise/Databases [https://perma.cc/LXZ5-JLKW].

129. Unlike flow "1", an international database center allows access not only to government authorities, but also to choke point private actors registered with IOs. For instance, INTERPOL, through its SLTD, collects information from member states and enables airlines, through its I-Checkit program, to query against the SLTD. *See* Shelley, *supra* note 3.

130. IOs work as database centers and allow access to the overall public, including choke point private actors. For instance, United Nations Security Council 1267 Committee collects information about terrorist organizations and individuals from member states and publicizes the list. *See* S.C. Res. 1267, (Oct. 15, 1999). INTERPOL, under its Notices program, collects information about wanted persons ("Red Notice") or persons presenting imminent threat ("Yellow Notice"), etc., and publicizes the list. The publications are made through the Internet, allowing access for the general public. *See* INTERPOL, *Notices*, http://www.interpol.int/INTERPOL-expertise/Notices [https://perma.cc/C9FT-5745].

131. A state's cooperation with another state generally depends on international or mutual legal assistance treaties ("MLATs") in which both states are members. However, contemporary MLATs generally do not provide international instantaneous sharing. The information under MLATs is reactively exchanged from one state to another for a specific crime under legal proceedings. It has a long process, going through multiple state authorities—a designated central state authority, diplomatic channels, and/or a state authority in charge of the requested information—of both the requesting and requested states with "duplicate checking of paperwork." Gail Kent, *The Mutual Legal Assistance Problem Explained*, THE CENTER FOR INTERNET AND SOCIETY (Feb. 23, 2015), http://cyberlaw.stanford.edu/blog/2015/02/mutual-legal-assistance-problem-explained [https://perma.cc/JM7A-GVGB]. Sometimes, the process is more complex when the "legislation requir[es] communication [to] be [made] via the traditional postal service." *Id.* ("The UN Cybercrime Study of 2013 indicates that most countries 'reported median response times of . . . 150 days for mutual legal assistance requests, received and sent . . . . It is clear that the use of formal cooperation mechanisms occurs on a timescale of months, rather than days.").

When there exist no such MLATs, the international laws imposing a "duty to report crime" instead provide a basis of mutual legal assistance and mutual law enforcement cooperation between states with no such mutual treaty. *See* UNCAC, *supra* note 18, art. 46(9)(a), 48(2). They generally follow the traditional purview of MLATs. Though they offer more instantaneous direct information exchange between state authorities for the early identification of the crime by detaching law enforcement cooperation from complicated mutual legal assistance, these exchanges of information are still reactive. *See id*. art. 46(1), (2), (13); art. 48(1)(a), (f).

However, there is an emergence of MLATs opting for proactive sharing regimes with less complicated, if not instantaneous, channels. For instance, the United States and Canada agreed to

5. Vulnerability Equity Process sharing the vulnerabilities in telecom or computer systems; Launching Automated Indicator Sharing based on 2015 Cyber Security Information Sharing Act[132]
6. Designation of terrorist organizations pursuant to Section 219 of the Immigration and Nationality Act; Designation of global terrorists under Executive Order (E.O.) 13,224; Public notification of sex offenders under the Sex Offender Registration and Notification Act[133]
7. Does not exist[134]

a. General public's obligation to report felonies pursuant to 18 U.S.C. § 4 (Misprision of Felony); Voluntary reporting with reward (Dodd-Frank or Qui Tam Act)

---

share visa and immigration information to allow immigration officers to "have timely access to current and accurate information" to "further the prevention, investigation, or punishment of acts that would constitute a crime." The Agreement Between the Government of Canada and the Government of the United States of America for the Sharing of Visa and Immigration Information, pmbl. & art. 2(b), U.S.-Can., Dec. 13, 2012, T.I.A.S. No. 13-1121. Regarding tax matters, the Nordic countries and the EU employed automatic information exchange to combat tax fraud and evasion. *See* Avtal om handräckning i skatteärenden, art. 11(1), http://www.norden.org/en/om-samarbejdet-1/nordic-agreements/treaties-and-agreements/taxation-affairs/avtal-om-handraeckning-i-skatteaerenden [https://perma.cc/C54Y-3VZD]; Directive 2014/107/EU of 9 December 2014 amending Directive 2011/16/EU as regards Mandatory Automatic Exchange of Information in the Field of Taxation, art. 1 (2), O.J. (L 359) 1 (2014). Furthermore, the OECD developed a global model of automatic exchange endorsed by the G20 with further expectation of full implementation at the global level. *See* OECD, *Standard for Automatic Exchange of Financial Account Information* 6 (2014), https://www.oecd.org/ctp/exchange-of-tax-information/automatic-exchange-financial-account-information-common-reporting-standard.pdf [https://perma.cc/68J8-P53Z].

132. This flow illustrates providing governmental information to choke point private actors, which is a principle to justify domestic "duty to report crime" law with criminal penalties. For instance, U.S. Homeland Security, under its Launching Automated Indicator Sharing program (based on the 2015 Cyber Security Information Sharing Act), allows choke point private actors to instantaneously access governmental information on threat indicators. *See* Mark Pomerleau, *DHS Stands up Public-Private Cyber Info Sharing Platform*, GCN (Mar 30, 2016), https://gcn.com/articles/2016/03/30/dhs-ais.aspx [https://perma.cc/ND7V-H6VW]; Brad S. Karp, *Federal Guidance on the Cybersecurity Information Sharing Act of 2015*, HARV. L. SCHOOL FORUM ON CORPORATE GOVERNANCE AND FIN. REGULATION (March 3, 2016), https://corpgov.law.harvard.edu/2016/03/03/federal-guidance-on-the-cybersecurity-information-sharing-act-of-2015/ [https://perma.cc/8KAC-PEGM]. The U.S. government, under Vulnerability Equity Process, disseminates the governmental information on vulnerabilities in telecom or computer systems to private sectors. *See* NAT'L SEC. AGENCY, *Commercial and Government Information Technology and Industrial Control Product or System Vulnerabilities Equities Policy and Process*, at 1 (Feb. 16, 2010) https://www.eff.org/files/2016/01/18/37-3_vep_2016.pdf [https://perma.cc/A4XK-ZW7F] ("This document establishes policy and responsibilities for disseminating information about vulnerabilities discovered by the United States Government (USG) or its contractors, or disclosed to the USG by the private sector or foreign allies in Government Off-The-Shelf (GOTS), Commercial Off-The-Shelf (COTS), or other commercial information technology or industrial control products or systems (to include both hardware or software).").

133. Some governmental information is publicized to the general public. For instance, the U.S. Department of Justice publicizes its list of terrorists and terrorist organizations. *See* The Immigration and Nationality Act, 8 U.S.C. § 1189(a)(1) (2004); *see also* Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001). In addition, in the United States, information about sex offenders is available to the public on the web. *See* Sex Offender Registration and Notification Act, 34 U.S.C. §§ 20901–20962 (2006).

134. Although this possible information flow would allow domestic choke point private actors direct access to foreign governmental information, no legal regime currently provides such access. However, if available, this channel would be the only one closest to the ideal international instantaneous sharing of information between government and private entities, as it does not need to go through any other intermediaries.

b. Financial institution's mandatory reporting of suspicious transactions to national authorities pursuant to 31 U.S.C. § 5318(g) and its corresponding regulations; Electronic communication service providers' and remote computing service providers' mandatory reporting of child pornography pursuant to 18 U.S.C. § 2258A; Voluntary reporting with reward (Dodd-Frank or Qui Tam Act); Voluntary reporting of cyber threat indicator under 2015 Cyber Security Information Sharing Act.

Each of the crime information flow-paths identified in Chart I has distinctive characteristics involving different levels of actors in information transmission. The successful instantaneous sharing of such information must meet three conditions: horizontal accountability, vertical accountability, and proportionality to privacy/reputational harm. Those three conditions are discussed in turn below.

i. Horizontal Accountability[135]

Sharing information at an international level is difficult due to the absence of a single supra-national government with control and command authority. Instead, individual states compete to safeguard their own national interests.[136] Formalized international information sharing seems even more difficult. Like individuals,[137] states are more likely to share information with other states when they are in an amicable, not conflicting, relationship. But relationships may change over time, depending on national interests. Thus, even when there is a present common interest in sharing national security information, the state will not share information if it fears defection.[138]

In contrast, institutionalist theorists argue that states voluntarily agree to be bound by promises made to other states, even in the absence of the

135. From the perspective of global governance, I adopt the term "horizontal accountability," often used in domestic governance research. *See* Guillermo A. O'Donnell, *Delegative Democracy*, 5 J. OF DEM. 55, 61 (1994) ("[A]ccountability runs not only vertically, making elected officials answerable to the ballot box, but also horizontally, across a network of relatively autonomous powers (i.e., other institutions) that can call into question, and eventually punish, improper ways of discharging the responsibilities of a given official.").

136. Anne L. Herbert, *Cooperation in International Relations: A Comparison of Keohane, Haas and Franck*, 14 BERKELEY J. INT'L L. 222, 226 (1996).

137. Claudia Toma & Fabrizio Butera, *Hidden Profiles and Concealed Information: Strategic Information Sharing and Use in Group Decision Making*, 35 PERS. SOC. PSYCHOL. BULL 793, 803–04 (2009) (illustrating that individuals with cooperative incentives are significantly more likely to pool unshared information with other team members than the individuals with competitive incentives); WOLFGANG STEINEL ET AL., THE GOOD, THE BAD AND THE UGLY THING TO DO WHEN SHARING INFORMATION: REVEALING, CONCEALING AND LYING DEPEND ON SOCIAL MOTIVATION, DISTRIBUTION AND IMPORTANCE OF INFORMATION 27 (2010) (describing that individuals are more likely to withhold or falsify information when they have noncooperative selfish motives).

138. JAMES IGOE WALSH, THE INTERNATIONAL POLITICS OF INTELLIGENCE SHARING, 47–48 (Colum. Univ. Press 2009).

supra-national government, for their shared interest. There are many interests that states share, "which in turn generate a demand for international institutions and rules that states will voluntarily agree to follow."[139]

Whether a realist or an institutionalist perspective is adopted, formalized information sharing at the international level with respect to crime is not a far-fetched idea. For all states, public security, as with public health and environment, is a public good to be protected. Similarly, crimes, as with epidemics and global warming, are public evils to be deterred. In this interconnected globalized world, public security "can only be provided efficiently at the international rather than national level."[140] Accordingly, states have voluntarily agreed to share certain crime information, such as DNA, fingerprints, and sexual exploitation images through INTERPOL with other states.[141] International treaties, described above as "duty to report crime" provisions, are manifestations of states' willingness to cooperate to achieve their common goals on crime detection and deterrence.

Yet, sharing crime information does not always coincide with a state's interests. For instance, states whose main source of economic interest originates from their strong bank secrecy laws might have a robust self-interest in not sharing suspicious transactions with other states.[142] Additionally, when crimes are committed by other states, it can be akin to a matter of national security. Considering that cyber-attacks are sometimes committed by states themselves,[143] the states where victims are located might have a strong interest in not sharing such information with

---

139. Herbert, *supra* note 136, at 226.

140. Martin Brookes & Zaki Wahhaj, *Global Public Goods Arguments for Collective Action*, INTERNATIONAL COUNCIL ON HUMAN RIGHTS POLICY 1 (2001), http://www.ichrp.org/files/papers/94/108_-_Global_Public_Goods_-_Arguments_for_Collective_Action_Brookes__Martin__Wahhaj__Zaki__2001.pdf [https://perma.cc/2SL7-7DNK].

141. *See* Interpol Databases, *supra* note 128.

142. Keen & Ligthart, *supra* note 76, at 86 (2004) ("Here the starting point is the observation that by providing information to foreign tax authorities a country makes itself less attractive to foreign investors—which can hardly be in its own best interests. Thus, as stressed by Tanzi and Zee (2001) in an early discussion of these issues, it is far from clear that information exchange agreements can be expected to be self-enforcing.").

143. *See* Ellen Nakashima et al., *U.S., Israel Developed Flame Computer Virus to Slow Iranian Nuclear Efforts, Officials Say*, WASH. POST (June 19, 2012), https://www.washingtonpost.com/world/national-security/us-israel-developed-computer-virus-to-slow-iranian-nuclear-efforts-officials-say/2012/06/19/gJQA6xBPoV_story.html?utm_term=.6f9c90bb5766 [https://perma.cc/XAD7-LM6Y]; US DEP'T OF DEF., *Department of Defense Cyberspace Policy Report*, at 9 (2011), https://fas.org/irp/eprint/dod-cyber.pdf [https://perma.cc/67BJ-Y55E] (declaring that cyber attacks could be considered acts of war); James A. Lewis & Katrina Tilmin, *Cyber Security and Cyberwar: Preliminary Assessment of National Doctrine and Organization*, CTR. FOR STRATEGIC AND INT'L STUDIES 3, http://unidir.org/files/publications/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf [https://perma.cc/2CVT-BKEY] (identifying 33 nations "includ[ing] cyberwarfare in their military planning and organization").

other states for national security reasons. States may also be unwilling to share information relating to crimes such as terrorism, in which political interpretation,[144] and states themselves, are involved.

In this context, as argued by the realists, a state might follow its self-interest by cheating others—obtaining more than the necessary information from others or providing less than the necessary information to others[145]—even if that state voluntarily agreed to be bound by the promise it made to share information. Scholars say, "international law has no life of its own, has no special normative authority . . . and there is no reason to expect states to comply with treaties when their interests and powers change."[146]

Accordingly, for this type of crime information, horizontal accountability—accountability to information sharing of other states—is a crucial element of the ideal regime for global regulation of a "duty to report crime" to overcome the realist arguments. Without horizontal accountability, in order for choke point private actors to access the required foreign governmental crime information, both governments giving and receiving information would have to rely on the honesty of the opposite government. That means, governments providing information believe that the information shared will not be used against them and the government receiving information relies on the honesty of the government providing the information. In the absence of mutual trust, state interest in withholding domestic crime information and cheating others is what directs the acts of states.[147]

Based on the foregoing analysis, this Article recognizes that an international body-centered structure, not a state-centered structure, needs to be employed. An international body-centered structure—information channel 1+2+3 and either 1, 2, or 3 in Chart I—needs to be established, not simply as a data center but as an independent supervisory body to secure horizontal accountability, thereby building trust between states and

144. An individual who is reproached as a terrorist in one state could be honored as a patriot in another state.

145. RAKESH AGRAWAL & EVIMARIA TERZI, *On Honesty in Sovereign Information Sharing*, *in* ADVANCES IN DATABASE TECHNOLOGY—EDBT 2006 240, 240 (Yannis Ioannidis et al. eds., 2006).

146. Jack L. Goldsmith & Eric A. Posner, *The Limits of International Law*, THE AM. ENTER. INST. FOR PUB. POL'Y RES. 3 (2005), http://www.angelfire.com/jazz/sugimoto/law.pdf [https://perma.cc/R7SL-TAX5].

147. The importance of state interest in determining whether to share information with other states is already explained above. *See* WALSH, *supra* note 138, at 47–48 (arguing that states share information based on state interest, rather than trust alone). However, this does not mean that trust between states, though not a sole conclusive factor, can be ignored. Scholars have cited trust as an important factor in information and knowledge sharing. *See, e.g.,* Kurt T. Dirks & Donald L. Ferrin, *The Role of Trust in Organizational Settings*, 12 ORG. SCI., 450 (2001); Niki Panteli & Siva Sockalingam, *Trust and Conflict Within Virtual Inter-Organizational Alliances: A Framework for Facilitating Knowledge Sharing*, 39 DECISION SUPPORT SYS. 599 (2005); Dale E. Zand, *Trust and Managerial Problem Solving*, 17 ADMIN. SCI. Q. 229 (1972).

overcoming the pursuit of states' individual self-interest.

In such a structure, it is predicted the information will be proactively shared with the foreign choke point private actors through an international body, which will manage access to the information in a way that eliminates the risk of abuse by foreign states. For example, in relation to information on state-sponsored cyber incidents, the attacked state tends not to share the information internationally, as it might expose the weak points in its cyber security, potentially damaging its national security interest. Although this concern is real, it is manageable. Contrary to information sharing of a state with the foreign choke point private actors directly through foreign states, where the source state of the information is meant to be exposed to foreign states, the international data center could choose not to disclose the source state of the information while providing the required information to foreign choke point private actors.

The risk of abuse by states could be further eliminated if the information at the international data center is provided directly to the choke point foreign private actors, rather than indirectly through foreign states, as in channel 2 in Chart I. For information that only choke point private actors find useful in detecting crime,[148] such as information on PEPs for financial institutions required to report suspicions of corruption, only the choke point private actors should have access to the data center while strictly prohibiting them from sharing such information with their government.

This role of an international data center should be supported by the role of an independent supervisory institution through regular inspections and penalization[149] of noncompliance to combat the mistrust between states by upholding horizontal accountability. It is crucial to encourage honesty "with an auditing device that checks at an appropriate frequency the integrity of the data submitted by the participants and penalizes by an appropriate amount the cheating behaviors."[150] If states are free to share only information that is preferential to them or to abuse the shared information for their own interests, trust between states will never be established.

---

148. Depending on the type of crime information, if the information shared, such as child pornography, does not pose a risk of harm to the states sharing the information and is necessary for crime investigation and prosecution, the international body may also provide state authorities direct access to such information.

149. Instead of imposing a penalty, carrots could be used to induce information sharing. For instance, information sharing for tax purposes could utilize such incentive mechanisms to make states exchange information. *See* Keen & Ligthart, *supra* note 76, at 88 ("[T]here is no intrinsic reason why some of the additional revenue collected as consequence of information exchange should not be transferred to the country that provides it."). However, it might be difficult to apply these tactics to crime information sharing, as deterrence of crime does not necessarily generate profits to be shared as an incentive with information providers.

150. AGRAWAL & TERZI, *supra* note 145, at 255.

Regular inspections and penalization of noncompliance, whether through soft or hard sanctions, would discourage states that voluntarily agree to share crime information from cheating to pursue their self-interest. Furthermore, it would also encourage non-member states to share crime information, thus coming closer to the ideal of international sharing. For instance, even with their soft law characteristics of non-binding power, FATF Recommendations backed by review and soft sanction penalties are widely adopted and implemented by member states and, more importantly, by non-member states.[151] The FATF policy of "naming and shaming" the Non-Cooperative Countries and Territories ("NCCTs")[152] and taking Recommendation 19 (formerly Recommendation 21) countermeasures[153] against NCCTs encourages member[154] and non-member states[155] to comply with its

151. FATF, FATF Steps up the Fight Against Money Laundering and Terrorist Financing (2012), http://www.fatf-gafi.org/publications/fatfrecommendations/documents/fatfstepsupthefightagainstmoneylaunderingandterroristfinancing.html [https://perma.cc/KH3H-Y3XY]. More than 180 governments, including thirty-five states and two regional organizations (European Union, Gulf Cooperation Council) as members, utilize FATF Recommendations as a global standard to combat money laundering and financing of terrorism. *Id.*

152. FATF, *About the Non-Cooperative Countries and Territories (NCCT) Initiative*, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/aboutthenon-cooperativecountriesandterritoriesncctinitiative.html?hf=10&b=0&s=desc(fatf_releasedate) [https://perma.cc/TE36-UE5Y]. This NCCT initiative was transformed into high-risk and non-cooperative jurisdictions in 2008, but it maintains generally the same framework. FATF, *High-Risk and Non-Cooperative Jurisdictions*, http://www.fatf-gafi.org/publications/high-riskandnon-cooperativejurisdictions/more/more-on-high-risk-and-non-cooperative-jurisdictions.html?hf=10&b=0&s=desc(fatf_releasedate) [https://perma.cc/C7NP-BLBR].

153. FATF, *International Standards on Combating Money Laundering and the Financing of Terrorism & Proliferation* 19 (Feb. 2012, updated Oct. 2016) [hereinafter *International Standards*], http://www.fatf-gafi.org/media/fatf/documents/recommendations/pdfs/FATF_Recommendations.pdf [https://perma.cc/4W22-5HJV].

> Financial institutions should be required to apply enhanced due diligence measures to business relationships and transactions with natural and legal persons, and financial institutions, from countries for which this is called for by the FATF. The type of enhanced due diligence measures applied should be effective and proportionate to the risks.Countries should be able to apply appropriate countermeasures when called upon to do so by the FATF. Countries should also be able to apply countermeasures independently of any call by the FATF to do so. Such countermeasures should be effective and proportionate to the risks.

Id.

154. JAE-MYONG KOH, SUPPRESSING TERRORIST FINANCING AND MONEY LAUNDERING, 162–63 (2006). The formal policy against member states is as follows:

> 1. Requiring the members to provide regular reports on their progress in implementing the Recommendations within a fixed timeframe;
> 2. Sending a letter from the FATF President to the relevant minister(s) in the member jurisdiction drawing their attention to non-compliance with the FATF Recommendations;
> 3. Arranging a high-level mission to the member jurisdiction in question to reinforce this message;
> 4. In the context of the application of Recommendation 21 by its members, issuing a formal FATF statement to the effect that a member jurisdiction is insufficiently in compliance with the FATF Recommendations; and,
> 5. Suspending the jurisdiction's membership of the FATF until the Recommendations have been implemented.

Id. (internal citations omitted).

155. The formal policy against non-member states is as follows:

Recommendations. The member states that were once subjected to the above measures, such as Turkey[156] and Austria,[157] proceeded to take necessary steps to implement the Recommendations. In 2000 and 2001, forty-seven jurisdictions were reviewed under the NCCTs process; twenty-three jurisdictions were identified as NCCTs.[158] However, since June 1, 2005, only Myanmar, Nauru, and Nigeria remained on the list.[159] Following the pressure from FATF, the three jurisdictions made genuine improvements to implement the FATF Recommendations, resulting in Nauru being delisted in October 2005, Nigeria in June 2006, and Myanmar in October 2006.[160] The OECD also takes similar measures against non-cooperative nations in tax matters.[161]

In contrast, a state-centered information sharing structure—information channels through flows 4 and 5, 6 or 7 of Chart I—whether a legal regime or not, is likely to fail to secure horizontal accountability and to provide the required crime information to choke point private actors. A state tends to withhold or distort the information for interrelated reasons: lack of trust, pursuit of self-interest, and a risk of information abuse by other states. Mutual review and inspection between states may curb these risks to some extent. However, in terms of cost, it would be a feasible or efficient solution for bilateral information sharing, but not for international information sharing, which this paper suggests as an ideal regime.

---

1. Actions to put an end to the detrimental rules and practices
   (i) Actions designed to encourage non-cooperative jurisdictions to adopt laws in compliance with FATF recommendations; and,
   (ii) Application of Recommendation 21
2. Counter-measures designed to protect economies against money of unlawful origin
   (i) Customer identification obligations for financial institutions in FATF members with respect to financial transactions carried out with or by individuals or legal entities whose account is in a "non-cooperative jurisdiction";
   (ii) Specific requirements for financial institutions in FATF members to pay special attention to or to report financial transactions conducted with individuals or legal entities having their account at a financial institution[] established in a "non-cooperative jurisdiction"; and,
   (iii) Conditioning, restricting, targeting or even prohibiting financial transactions with non-cooperative jurisdictions.

Id. at 164–65 (internal citations omitted).

156. *See* FATF, *Annual Report: 1996–1997, Financial Action Task Force on Money Laundering, Monitoring the Implementation of Anti-Money Laundering Measures* 10–11 (June 1997) http://www.fatf-gafi.org/media/fatf/documents/reports/1996%201997%20ENG.pdf [https://perma.cc/3NAE-WFG6].

157. FATF, *Annual Report: 1999–2000, Financial Action Task Force on Money Laundering, Improving Members' Implementation of the Forty Recommendations* 20–22 (June 22, 2000) http://www.fatf-gafi.org/media/fatf/documents/reports/1999%202000%20ENG.pdf [https://perma.cc/4XQ6-7P7N].

158. KOH, *supra* note 154, at 165.

159. *Id.*

160. FATF, *Annual Review of Non-Cooperative Countries and Territories 2006–2007: Eighth NCCT Review* 2 (Oct. 12, 2007) http://www.fatf-gafi.org/media/fatf/documents/reports/2006%202007%20NCCT%20ENG.pdf [https://perma.cc/Y7EX-FGZK].

161. *See* Keen & Ligthart, *supra* note 76, at 102–03 ("In April 2002, the OECD published a blacklist of seven noncooperative tax havens not willing to enter such commitments, against which OECD members had reserved the right to undertake *defensive measures*.") (emphasis in original).

Furthermore, the lack of an enforceable penalty of a state over non-compliant states will direct states to behave by following the logic of state interest rather than legal agreements.

ii. Vertical Accountability

When the governmental crime information shared with choke point private actors is the outcome of administrative discretion, which affects the rights or interests of the subjects whose information is shared, it is an administrative decision that should ensure accountability—vertical accountability—to the subjects affected. For some of the governmental crime information shared that is described below, an administrative agency exercises its discretion in establishing the information.

Governmental crime information about past crimes that have been previously decided and reviewed by the judiciary generally does not provide room for discretion to regulatory bodies. For example, in the United States, information about the name, current location, and past offenses of sex offenders is shared with choke point private actors through publication on a government website, as long as the offenders are convicted of the sex offenses specified under the Sex Offender Registration and Notification Act.[162] Many other states have adopted similar laws.[163] Judicial review determines the information that should be shared with the public, which certainly includes choke point private actors.

In addition, the governmental crime information reported by the victims of crime about objective facts does not require any further administrative discretion for it to be shared with choke point private actors. When U.S. passports are reported lost or stolen, they are added to an electronic database after a formal verification for accuracy by comparing the information stored in the Passport Information Electronic Records System owned and operated by the Bureau of Consular Affairs.[164] The victim choke point private actors participating in the Automated Indicator Sharing under the 2015 Cyber Security Information Sharing Act share their information on cyber threat indicators with other participating choke point private actors managed through a Department of Homeland Security ("DHS") system in the Department's National Cybersecurity and Communications Integration Center. The indicators are not validated by DHS.[165]

---

162. 34 U.S.C. §§ 20901–62 (2017).

163. *See generally* Global Overview of Sex Offender Registration and Notification Systems, OFF. OF SEX OFFENDER SENTENCING, MONITORING, APPREHENDING, REGISTERING, AND TRACKING (Apr. 2014), http://www.smart.gov/pdfs/GlobalOverview.pdf [https://perma.cc/49CP-687H].

164. *Privacy Impact Assessment: Online Passport Lost & Stolen System*, DEPT. OF STATE 2 (2008), https://www.state.gov/documents/organization/242420.pdf [https://perma.cc/T8BN-5GLX].

165. *Automatic Indicator Sharing (AIS)*, US-CERT, https://www.us-cert.gov/ais

Other governmental crime information tends to be the subject of administrative discretion. In the United States, a list of foreign terrorist individuals or organizations is created by the Secretary of State or the Secretary of the Treasury based on the governmental crime information.[166] This list typically includes both classified and open source information that names the foreign individuals or entities that have committed, or pose a significant risk of committing, acts of terrorism threatening the security of U.S. nationals or national security, foreign policy, or the U.S. economy.[167] Cyber child pornography clearinghouses, such as The National Center for Missing & Exploited Children ("NCMEC") in the United States,[168] review and verify the images of cyber child pornography listed by the ISPs, who usually are third parties in relation to the crime, before handing the images over to the law enforcement agencies and sharing this with other choke point private actors.[169]

This discretionary decision made by the administrative agency does not simply assist choke point private actors in providing better crime detection, but also aids in deciding who should be the subject of greater scrutiny by the choke point private actors, thus affecting the rights or interests of the subject of the shared information.

Regulation of a "duty to report crime" generally only triggers a reporting duty to verify the crimes that are suspected. However, states often impose an obligation to deny service to the suspicious individuals or entities to deter further crimes. Thus, when a government shares its crime information, the private sector actor will deny its services to the subjects

---

[https://perma.cc/8DAA-LVHD].

166. Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 25, 2001).

167. *Id.*

168. Appellant Opening Brief at 14, United States v. Ackerman, 831 F.3d 1292 (10th Cir. 2016) (No. 14-3265). Depending on the state, the child pornography information clearing house is established either as a governmental organization or non-governmental organization. However, even non-governmental clearing houses, such as NCMEC, are funded in part by federal grants and authorized by federal law to work as a government agent through its partnership with government. United States v. Keith, 980 F. Supp. 2d 33, 38–39 (D. Mass. 2013); *see also Programs and Services*, THE NAT'L CENT. FOR MISSING & EXPLOITED CHILDREN, http://www.missingkids.com/Programs [https://perma.cc/73NG-MTVE]. More importantly, a U.S. court recently decided that NCMEC is a government agency, not a private entity. United States v. Ackerman, 831 F.3d 1292, 1296–98 (10th Cir. 2016) ("Focusing in particular on NCMEC's CyberTipline functions . . . illustrates and confirms the special law enforcement duties and powers it enjoys . . . . [S]o much law and evidence suggest[s] NCMEC qualifies as a governmental entity."). Besides, these non-governmental clearing houses sometimes have access to governmental databases, as the Internet Watch Foundation ("IWF") of UK does by making hash lists from the images from the Home Office's new Child Abuse Image Database ("CAID"), not just from public reporting or reporting from ISPs. Accordingly, this Article categorizes the information of these clearing houses for child pornography as governmental information. *See Hash List "Could be Game-Changer" in the Global Fight Against Child Sexual Abuse Images Online*, INTERNET WATCH FOUND. (Aug 10, 2015) https://www.iwf.org.uk/about-iwf/news/post/416-hash-list-could-be-game-changer-in-the-global-fight-against-child-sexual-abuse-images-online [https://perma.cc/AD9P-6P2F].

169. Appellant Opening Brief, *supra* note 168, at 14.

of the information, based on the information shared. In relation to child pornography, some jurisdictions (e.g. Austria,[170] Germany,[171] Spain,[172] and Taiwan[173]) require ISPs to remove or disable access to illegal content.[174] Therefore, when the governmental information about child pornography (e.g. hash values of child pornography or a list of URLs of child pornography websites) is shared with its ISPs, the ISPs will remove or disable access to the content solely based on the shared information, thereby encroaching on the rights or interests of the content owners.[175]

Without such a duty, choke point private actors tend not to take a risk of dealing with the subjects of the shared governmental crime information, thus making it difficult, if not impossible, for them to enjoy their rights or interests. Although the United States generally does not impose a duty to remove or disable access on ISPs,[176] the ISPs voluntarily do so. Their terms of service generally give ISPs the right to remove and disable access to illegal content, and ISPs voluntarily exercise this right against cyber child pornography.[177] In the United States, the NCMEC agreed "to use

---

170. Bundesgesetz, mit dem bestimmte rechtliche Aspekte des elektronischen Geschäfts- und Rechtsverkehrs geregelt werden [Federal Act Governing Certain Legal Aspects of Electronic Commercial and Legal Transactions], BGBI. I Nr. 152/2001 § 16(1)2 (Dec. 21, 2001) (Austria) https://www.ris.bka.gv.at/Dokumente/Erv/ERV_2001_1_152/ERV_2001_1_152.pdf [https://perma.cc/TS4U-8ELN].

171. The Telemediengesetz [the Telemedia Act], EGRL 179/2007, Abschnitt 3 § 10 (Feb. 26, 2007) (Ger.) https://www.gesetze-im-internet.de/tmg/__10.html [https://perma.cc/4M3L-8LFJ].

172. De Servicios de la Sociedad de la Informacion y de Comercio Electronico [The Information Society and Electronic Commerce Services Law], Ley 34/2002, art. 16(1)(a) (July 11, 2002) (Spain), http://www.wipo.int/wipolex/en/text.jsp?file_id=268430 [https://perma.cc/FQ93-Q4SF].

173. Regulations for the Rating of Internet Content, GIO Press Release 0930622071-A, art. 8 (Apr. 26, 2004) (Taiwan) http://www.ncc.gov.tw/english/files/10092/68_572_100923_1.pdf [https://perma.cc/NW4H-YNCG].

174. Weixiao Wei, *Online Child Sexual Abuse Content: The Development of a Comprehensive, Transferable International Internet Notice and Takedown System*, INTERNET WATCH FOUND. 98 (2011), https://www.iwf.org.uk/sites/ . . . [https://perma.cc/87ZZ-VXUR].

175. A research study experimented how ISPs react to the complaints about alleged copyright infringement on a website that actually contained perfectly legal material. In the case of UK ISPs, they "took the site down almost immediately *effectively censoring* . . . legal content without investigation." Christian Ahlert et al., *How 'Liberty' Disappeared from Cyberspace: The Mystery Shopper Tests Internet Content Self-Regulation* 3 (2004) (emphasis in original), http://pcmlp.socleg.ox.ac.uk/wp-content/uploads/2014/12/liberty.pdf [https://perma.cc/5DQC-CP76]; *see also* Richard Clayton, *Judge & Jury? How "Notice and Take Down" Gives ISPs an Unwanted Role in Applying the Law to the Internet* (July 26, 2000), http://www.cl.cam.ac.uk/~rnc1/Judge_and_Jury.html [https://perma.cc/9LCX-JDCX] ("[Notice and Take Down] can lead to injustices as lawful material is censored because ISPs cannot take the risk that a court will eventually agree that it can indeed remain available.").

176. Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001). In the case of Pennsylvania, the state law imposes the duty to remove or disable access when on notice by the Attorney General. 18 PA. CONS. STAT. § 7622 (2014). In addition, the notice is not a pure administrative discretionary decision. *Id.* It has to be reviewed by the court, as it requires the Attorney General to obtain the order from the court. *Id.*

177. Most ISPs seem to reserve the right to remove illegal content. *See*, *e.g.*, *Privacy & Terms*, GOOGLE, https://www.google.com/intl/en/policies/terms/ [https://perma.cc/SU2G-23UR] ("We may review content to determine whether it is illegal or violates our policies, and we may remove or refuse to display content that we reasonably believe violates our policies or the law."); *Terms of Use*, VERIZON, http://www.verizon.com/about/terms-conditions/terms-of-use [https://perma.cc/L6AU-W5TP] ("We reserve the right to: (a) use, copy, display, store, transmit and reformat data

NCMEC's database of web sites to identify those containing child pornography and to then allow any cable operator that owns or controls a server used by the site to shut it down."[178] The three biggest ISPs in the world, Verizon, Time Warner Cable, and Sprint, have agreed "to purge their servers of all child pornography Web sites identified by the [NCMEC]."[179]

Similarly, financial institutions, working from the list of individuals and entities designated as terrorists by the government, not only report suspicious activities to government authorities, but also freeze their assets. Unlike child pornography, this duty to freeze is imposed by international law[180] as well as domestic laws.[181]

Administrative laws require the discretion of government agencies to be exercised "in a manner that is informed and responsive to the wide range of social and economic interests and values affected by their decisions,"[182] which can be described here as vertical accountability, through legal procedures and judicial review. The ex-ante mechanism is that states usually allow people to participate in rule-making procedures through a notice-and-comment procedure.[183] The ex-post mechanism is that judicial review by the courts of the administrative decision is available to the adversely affected parties.[184]

However, with the emergence of global regulatory regimes, "the vast increase in the reach and forms of transgovernmental regulation and administration designed to address the consequences of globalized interdependence"[185] has created an accountability vacuum at the international level. "[P]olitical and legal accountability and control that would apply to purely domestic regulatory measures" are absent from the global regulatory decisions.[186] This lack of accountability damages the legitimacy of the global regulatory regimes, "since public exercises of

---

transmitted over our network and to distribute such content to multiple Verizon servers for back-up and maintenance purposes; and (b) block or remove any unlawful content you store on or transmit to or from any Verizon server.").

178. News Report, *Attorney General Lynch to Remove Child Pornography Sites from the Internet*, GOV'T TECH. (July 23, 2008) http://www.govtech.com/security/Attorney-General-Lynch-to.html [https://perma.cc/RXQ2-6PQX].

179. News Report, *Leading ISPs Reach Agreement to Block Child Pornography*, GOV'T TECH. (June 10, 2008) http://www.govtech.com/security/Leading-ISPs-Reach-Agreement.html [https://perma.cc/W4YF-QR59].

180. *See, e.g.*, S.C. Res. 1267, ¶ 4(b) (Oct. 15, 1999); S.C. Res. 1989, ¶ 1(a) (June 17, 2011); S.C. Res. 2253, ¶ 2(a) (Dec. 17, 2015).

181. Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001); 18 U.S.C. § 2339B(a)(2).

182. Richard B. Stewart, *U.S. Administrative Law: A Model for Global Administrative Law?*, 68 LAW & CONTEMP. PROBS. 63, 75 (2005).

183. *Id.* at 81.

184. *Id.* at 85.

185. Benedict Kingsbury et al., *The Emergence of Global Administrative Law*, 68 LAW & CONTEMP. PROBS. 15, 16 (2005).

186. Stewart, *supra* note 182, at 69.

power are lawful on condition that they do not violate these values and principles."[187]

The suggested ideal legal regime for a "duty to report crime" is a type of global regulatory regime that allows an administrative decision made in one state to be applied in another state through the principle of mutual recognition.[188] As with domestic governmental crime information, crime information decided by a foreign administrative body and shared with choke point private actors will affect the rights or interests of the individuals whose information is shared.

This creates a risk of "short-circuiting the role of domestic administrative law"[189] in securing vertical accountability. In order for global regulation of a "duty to report crime" to effectively eliminate the above risk, it is submitted there should be an international supervisory body as an implementer[190] to secure both ex-ante and ex-post vertical accountability, as in domestic administrative law.

Ex-ante vertical accountability may be established through "intergovernmental regimes of administrative law standards and mechanisms to which national administrations must conform."[191] Intergovernmental regimes monitor and review the state's implementation of the procedural standards through mutual evaluation or periodic on-site inspection.[192]

The concern is that a foreign administrative decision may have been made without following the same administrative law principles of the state where its decision takes effect, thus rendering it invalid if it were made in the affected state. The French Conseil d'Etat ruled against the lawfulness of an entry on the SIS that had been made by another Member State, Germany, because Germany failed to provide sufficient information for the claimant regarding the listing of claimants in the Schengen system.[193]

To obtain ex-post vertical accountability, a "top-down approach" of global regulatory procedure is to be actualized by the international supervisory body.[194] Although this demand for judicial review of global regulatory regime is expected to be met with the "bottom-up approach"—

187. David Dyzenhaus, *The Rule of (Administrative) Law in International Law*, 68 LAW & CONTEMP. PROBS. 127, 147 (2005).

188. Kalypso Nicolaidis & Gregory Shaffer, *Transnational Mutual Recognition Regimes: Governance Without Global Government*, 68 LAW & CONTEMP. PROBS. 263, 268 (2005) (suggesting the use of the mutual recognition principle as to govern the recognition of foreign laws, regulations, and standards among states).

189. Stewart, *supra* note 182, at 70.

190. Nicolaidis & Shaffer, *supra* note 188, at 282.

191. Kingsbury et al., *supra* note 185, at 16.

192. *Id.*

193. Elspeth Guild, *Moving the Borders of Europe*, U. OF NIJMEGEN, at 26 (May 30, 2001), http://cmr.jur.ru.nl/cmr/docs/oratie.eg.pdf [https://perma.cc/FR33-BSJE].

194. Stewart, *supra* note 182, at 72.

the extension of existing domestic administrative law principles[195]—as in the Hamssaoui and Forabosco case,[196] a "top-down approach," especially for the international regulatory network or body where judicial review is absent, also continues to be developed.[197]

For instance, the Security Council Resolution 1267 Committee is responsible for compiling a consolidated list of terrorist individuals and entities based on the information supplied by states.[198] "The listing mechanism can have far-reaching domestic consequences."[199] Not only the state requesting the listing but also all the other states are required to sanction the individuals or entities listed.[200] The 1267 Committee provides a procedure for the listed individuals and entities to make a direct petition and review request for delisting to the Office of the Ombudsperson of the Committee instead of the courts in all member states where their interests are affected.[201]

For this purpose, among the channels of the proposed contemporary architecture of international top-down vertical cooperation, this Article suggests that an international body-centered structure—information channel 1+2+3 and either 1, 2, or 3 in Chart I—should be employed, not a state-centered structure—information channels through 4, 5, 6, or 7 of Chart I.

Ex-ante vertical accountability can only be accomplished by an international body-centered structure, as the state-centered structure lacks an international centralized body to implement and supervise the administrative standard and mechanism. Although it is true that ex-post vertical accountability seems to be secured in both structures, through a "bottom-up approach" in the state-centered structure and a "top-down approach" in the international body-centered structure, the latter seems to be more appropriate. While the rights and interests of the subjects of the shared information will be affected internationally, as in the listings of the 1267 Committee, the effect of a "bottom-up approach" to secure vertical accountability is limited only to the bottom local jurisdiction. Under the latter approach, judicial review needs to be pursued in each individual jurisdiction where the subject of the shared information aims to recover his impinged interests or rights. Even if an international body-centered

195. *Id.* at 107.
196. Guild, *supra* note 193, at 26.
197. Kingsbury et al., *supra* note 185, at 57; *see also* Stewart, *supra* note 182, at 88–100.
198. S.C. Res. 1267, ¶ 4(b) (Oct. 15, 1999).
199. Dyzenhaus, *supra* note 187, at 141.
200. S.C. Res. 1267, ¶ 4(b) (Oct. 15, 1999). Referring to Committee 1267's adopted Resolution 1373, "all States shall take certain actions against the financing of terrorist activities, among other actions." Dyzenhaus, *supra* note 187, at 141 (internal quotations omitted).
201. *The Office of the Ombudsperson to the ISIL (Da'esh) & Al-Qaida Sanctions Committee*, UN (2017) https://www.un.org/sc/suborg/en/ombudsperson [https://perma.cc/4GRE-VAYR].

structure adopts a "bottom-up approach," the outcome of a judicial review in a home state that upholds the rights and interests of the subject of the shared information involves difficult and complicated procedures in order for it to be acknowledged in other states. For example, before reformation of the 1267 Committee to its current "top-down approach," the persons listed by the Committee had to challenge the listing in a domestic court, and then go through a further complicated process at the international level.[202]

iii. Proportionality of Harm to Privacy and Reputation

The third and final element of the ideal regime is the requirement to consider proportionality to privacy/reputational harm. Some governmental crime information shared with private choke point actors could create a risk for two different but interrelated protected values: the privacy right of the subject of the information and the subject's reputation, thus, further negatively affecting his or her business.[203] Though interrelated,[204] the two values are not attached to one another. When the subject of the shared information is a private entity, such entities have no privacy right.[205] However, their reputation and interests that are damaged by the shared information should still be considered.

The right to privacy is protected by states across the globe as a human right. The International Covenant on Civil and Political Rights ("ICCPR"), which has been ratified by 167 states, provides that "[n]o one shall be subjected to arbitrary or unlawful interference with his privacy" and "[e]veryone has the right to the protection of the law against such interference or attacks."[206] The EU has clearly articulated the right to privacy under the European Convention for the Protection of Human

---

202. See E. Alexandra Dosman, For the Record: Designating "Listed Entities" for the Purposes of Terrorist Financing Offenses at Canadian Law, 62 U. TORONTO FAC. OF L. REV. 1, 13 (2004). In discussing the Guidelines established for the 1267 Committee, another author states:

> An individual or organization that has been listed cannot apply to be delisted. A listed person must petition his or her home country to request a review of the case, and the home country then acts as the person's advocate if the review is favorable. The home country has to approach the government requesting the listing and attempt to persuade it to submit a joint or separate request to the Security Council for delisting. The home country can then submit the request even if the other government does not agree, but every member of the committee has an effective veto on any request. If the committee cannot achieve consensus, then the matter is remitted to the Security Council for final decision-making.

Dyzenhaus, *supra* note 187, at 141 n.60 (citing *Dosman*, *supra*).

203. *See* Kang, *supra* note 1, at 395, 399.

204. International Covenant on Civil and Political Rights art. 17, Dec. 16, 1966, 6 I.L.M. 368 (1967) [hereinafter International Covenant] (discussing protection of "privacy" together with protection from unlawful attack on "honour and reputation").

205. *See* FCC v. AT&T Inc., 562 U.S. 397 (2011) (holding that corporations do not have "personal privacy" for the purposes of FOIA Exemption 7(C)); see also Robert Barnes, Do Companies Have "Personal Privacy" Rights?, WASH. POST (Jan. 20, 2011), http://www.washingtonpost.com/wp-dyn/content/article/2011/01/19/AR2011011907414.html [https://perma.cc/BE4L-WTTJ].

206. International Covenant, *supra* note 204, art. 17(1)–(2).

Rights and Fundamental Freedoms ("ECHR") as a human right that should be protected.[207] Although the U.S. Constitution does not specifically mention the right to privacy, the Constitution has been interpreted by the courts, including the U.S. Supreme Court, as providing for that right.[208]

With the development of communication technology and an age where the rapid and widespread movement of information is now the norm, international society has recognized the importance of the protection of informational privacy.[209] Information about oneself can have serious effects on an individual's life. Though the right to privacy is difficult to define,[210] this Article regards it as an individual's right to control personal information with regards to both (1) types of information and (2) manners of distribution and sharing of that information.

As for types of information, the right to privacy is not an absolute right. Although Article 17 of the ICCPR does not contain a permissible limitation clause, the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression ("Special Rapporteur") recognizes permissible limitations on the right to privacy, stating that the right is subject to necessary, legitimate, and proportionate restrictions.[211] Under the ECHR, the EU provides the exceptions where privacy could be conceded: "[for] the interests of national security, public safety or the economic well-being of the country, for the prevention of disorder or crime, for the protection of health or morals, or for the protection of the rights and freedoms of others."[212]

Accordingly, depending on the content of the crime information possessed by the government, the privacy right of an individual may be restricted to various degrees. If the governmental information concerns crimes that are serious or have been reviewed by the court, the right to privacy is not likely to prevent public dissemination of that information. For example, while information about terrorists is likely to be shared with the public even without judicial review, information about sex offenders involving crimes against children may be shared with the public after a

---

207. European Convention for the Protection of Human Rights and Fundamental Freedoms, 4 November 1950, ETS 5, art. 8, [hereinafter European Convention] http://www.echr.coe.int/Documents/Convention_ENG.pdf [https://perma.cc/B2JS-7A8T].

208. *See* Griswold v. Connecticut, 381 U.S. 479, 484–85 (upholding the right to privacy in marriage even when the right is not expressly protected under the First Amendment).

209. *The Right to Privacy in the Digital Age*, OHCHR, http://www.ohchr.org/EN/Issues/DigitalAge/Pages/DigitalAgeIndex.aspx [https://perma.cc/XB7U-Y2FE].

210. W. A. Parent, *A New Definition of Privacy for the Law*, 2 LAW & PHIL. 305, 305 (1983).

211. Frank La Rue, *Report of the Special Rapporteur on the Promotion and Protection of the Right to Freedom of Opinion and Expression*, UN HUMAN RIGHTS COUNCIL, A/HRC/23/40, at 8 (2013), http://www.ohchr.org/Documents/HRBodies/HRCouncil/RegularSession/Session23/A.HRC.23.40_EN.pdf [https://perma.cc/R5QL-NZEV].

212. European Convention, *supra* note 207, art. 8(2).

judicial review. On the other hand, information concerning less serious crimes not reviewed by the court, such as PEP information as a risk indicator to deter corruption, might have stronger, but not complete, protection of the right to privacy.

Additionally, even when a legitimate expectation of an individual exists that the governmental information about him or her will not be disclosed, establishment of proportional manners of distribution and sharing, as explained below, could overcome the privacy right protection. Regarding disclosure of the public record (e.g. governmental crime information), in many cases, U.S. courts have allowed the disclosure of information if certain conditions are met: "(1) . . . the party [has] a legitimate expectation that the materials or information will not be disclosed[;] (2) . . . disclosure [is] nonetheless required to serve a compelling state interest[;] (3) . . . the necessary disclosure [will] occur in that manner which is least intrusive with respect to the right to confidentiality."[213] In recognizing this permissibility of limiting privacy, the Special Rapporteur required that "[r]estrictive measures . . . must be appropriate to achieve their protective function, they must be the least intrusive instrument amongst those which might achieve the desired result, and they must be proportionate to the interest to be protected."[214]

This proportionality can be attained through appropriate procedures to restrict distribution of the information with the help of technical solutions. For instance, INTERPOL allows the airlines participating in its I-Checkit border screening system to query the SLTD database, not by accessing the raw data directly, but by using the information provided by the allegedly suspicious client, thus eliminating the risk of privacy breaches.[215] Further, the SLTD database only includes a travel document number, the form of a document, and country code, not the personal data.[216] At the domestic level, in the case of the United States, technical solutions are being employed to help eliminate child pornography on the Internet. Thus, information about child pornography can be shared with choke point private actors through the Hash Value Sharing Initiative of the NCMEC, as a centralized data center, without worrying about potential privacy breaches. This is because the NCMEC does not provide the child pornography images, but only their representative "MD5 hash values."[217]

---

213. Jones v. Jennings, 788 P.2d 732, 738 (Alaska 1990) (quoting Martinelli v. District Court, 612 P.2d 1083, 1091 (Colo. 1980)).

214. La Rue, *supra* note 211, at 9.

215. *AirAsia Becomes First Airline to Pilot INTERPOL I-Checkit*, INTERPOL (May 13, 2014), http://www.interpol.int/News-and-media/News/2014/N2014-082 [https://perma.cc/6V3E-AEUX].

216. *Id.*

217. Sean Gallagher, *Updated: How Verizon Found Child Pornography in its Cloud*, ARS TECHNICA (Mar. 5, 2013), https://arstechnica.com/information-technology/2013/03/how-verizon-found-a-child-pornographer-in-its-cloud/ [https://perma.cc/XZJ6-NVMQ].

This means that choke point private actors can detect and confirm whether the pornography they encounter in the course of their business is child pornography that needs to be reported.

Apart from the right to privacy, preservation of reputation is crucial, especially when the private entities that are not protected by privacy rights[218] are victims of the crime whose information is shared. Disclosure of such information about private entities as victims of crime damages their reputations, thus significantly affecting their business outcomes.[219] Such a risk of reputational harm, particularly against a private entity who reported the information as a victim to the government, would prevent private entities from reporting to the government.[220]

With regards to such governmental crime information, it is recommended that disclosure be allowed to the greatest extent possible, provided that technical solutions are used to ensure appropriate procedures and restrictions are in place to control distribution of the information and preserve the reputation of victim private entities. In the United States for example, the Department of Defense's cyber incidents information, which might cause reputational harm to the victim, is shared only with strictly limited authorized choke point private actors.[221] In addition, the information is shared only to the extent necessary for detection and deterrence of a cyber incident, and there is a requirement to minimize the information that can identify the victim of the cyber incident.[222] Similarly, the Automatic Indicator Sharing of the DHS does not disclose the identity of the source of those shared cyber incident indicators to other participants without affirmative consent.[223] For this purpose, the DHS employs strict measures and processes, which are regularly tested.[224]

Overall, in relation to governmental crime information that potentially encroaches on the privacy rights or reputational interest of the subject of the information when shared, the disclosure should be limited in proportion to the legitimate aims of disclosure, with the use of procedural

---

218. *See* FCC v. AT&T Inc., 562 U.S. 397 (2011); Preamble, *International Covenant on Civil and Political Rights,* UN HUMAN RIGHTS ("[r]ecognizing that these rights derive from the inherent dignity of the human person").

219. *See generally Cyber Thieves Looking for Their Next Target*, BLUEFIN (Dec. 9, 2015), https://www.bluefin.com/bluefin-news/cyber-thieves-looking-for-their-next-target/ [https://perma.cc/T629-SFCB] (explaining the total expenses incurred by the 2013 Target data breach).

220. *See* Kang, *supra* note 1, at 399.

221. *See* The National Defense Authorization Act for Fiscal Year 2013, § 941(C)(3); *see also* 32 C.F.R. § 236.4(m)(1)–(4) (2015).

222. *See* 32 C.F.R. § 236.4(l) (2015); 32 C.F.R. § 236.2 (2015).

223. US-CERT, *supra* note 165.

224. *Id.* ("AIS has processes which: Perform automated analyses and technical mitigations to delete PII that is not directly related to a cyber threat; Incorporate elements of human review on select fields of certain indicators to ensure that automated processes are functioning appropriately; Minimize the amount of data included in a cyber threat indicator to information that is directly related to a cyber threat; Retain only information needed to address cyber threats; and Ensure any information collected is used only for network defense or limited law enforcement purposes.").

and technical measures to minimize the extent and scope of disclosure.

Accordingly, when choke point private actors rely on governmental crime information that has been made freely available to the public—information channels 3 and 6 in Chart I—unlike that shared only with choke point private actors—information channels 1, 2, 4, 5, and 7 in Chart I—the information shared is circumscribed by strict standards that exist to protect privacy and reputational harm. In other words, the shareable information is limited to past crimes, which are either serious or have been reviewed by the courts. As properly demonstrated by Chart I, the information available to choke point private actors through the public—information channels 3 and 6—is about terrorist organizations and individuals,[225] wanted suspects who have committed serious crimes that satisfied the minimum penalty threshold,[226] or sex offenders against children.[227]

However, this limited governmental crime information, which is at the same level of access as the public, fails to provide choke point private actors with enough of the required crime information to carry out their "duty to report crime" imposed by the government. Many times, choke point private actors need information about crime that is less serious and not proven to be committed. Information such as cyber incidents or breaches that should be shared with choke point private actors to further detect and deter such crimes cannot be shared by making them available to the public because of the possible reputational harm to the victim entities.[228]

Thus, to create the ideal regime, the governmental crime information made available to the public—information channels 3 and 6 in Chart I—is a necessary but not sufficient condition. The sufficient condition is satisfied by sharing governmental crime information only with choke point private actors—information channels 1, 2, 4, 5, and 7 in Chart I.

C. Practical Model for The Ideal Regime

Three criteria—horizontal accountability, vertical accountability, and proportionality to privacy/reputational harm—are suggested for some but not all top-down cooperations. Horizontal accountability is required for information that triggers conflicts of interest between states, thus causing states to cheat each other; vertical accountability should be required for

225. *See* S.C. Res. 1267 (Oct. 15, 1999); The Immigration and Nationality Act, 8 U.S.C. § 1189(a)(1) (2004); Exec. Order No. 13,224, 66 Fed. Reg. 49,079 (Sept. 23, 2001).

226. *See* INTERPOL, *Notices*, http://www.interpol.int/INTERPOL-expertise/Notices [https://perma.cc/C9FT-5745].

227. 42 U.S.C. §§ 16901–62; *see also* OFFICE OF SEX OFFENDER SENTENCING, *supra* note 163.

228. Kang, *supra* note 1, at 399–400.

information established under the administrative discretion and which invades the rights and interests of the subjects of the shared crime information; finally, proportionality should be required for information that encroaches on the right to privacy or reputation of the subjects of the shared information.

To satisfy each criterion required by types of crime information shared, the ideal regime for top-down cooperation should accordingly be established as illustrated above. If global regulation of a "duty to report crime" requires top-down cooperation, which will encompass all types of information, the regime should satisfy all three criteria.

As illustrated earlier, in relation to vertical and horizontal accountability, state centered information channels 4, 5, 6 or 7 in Chart I, are likely to fail to satisfy these three requirements. Regarding the proportionality to privacy/reputational harm, information channels 3 and 6 in Chart I, where choke point private actors access the publicized governmental crime information, are limited to information on past and serious crimes.

Accordingly, the one-size-fits-all regime should follow information channel 2 in Chart I. A global regulatory body should be established that would function as an international data center to consolidate the governmental crime information and grant choke point private actors direct access. It would also act as a supervisory body to review the substance of the shared information and procedures of information production with the authority to penalize noncompliance. Under this common structure, specific procedures and technical solutions, such as query-hit or direct access to raw data, would be implemented to allow choke point private actors to access the database in the least intrusive manner. The access would be differentiated based on the types of information shared.

This one-size-fits-all regime of governmental crime information sharing with choke point private reporters may not necessarily be a farfetched idea, but simply one that is in an embryonic stage. Moreover, INTERPOL, which has consolidated diverse types of governmental crime information as a data center, could be the best possible choice for such a regime on the condition that the supervisory role is expanded to meet the three criteria discussed above.

INTERPOL took the initiative of opening its SLTD database, one of its many crime information databases, to authorized choke point private actors under the I-Checkit program. Although it is currently only for airlines, it plans to expand the scope of choke point private actors to

include the hotel, banking, and maritime transportation sectors.[229] Considering that these choke point private reporters of I-Checkit have no "duty to report crime," there is a stronger rationale to allow the choke point private actors that have a "duty to report crime" to access requisite INTERPOL databases.

Global regulations that establish a "duty to report crime" could designate this INTERPOL database to be utilized as a platform for governmental crime information sharing with choke point private actors, just as the UNNDPS recommends member states to use INTERPOL databases as a platform of police information sharing.[230] Alternatively, it could also be supported by the UN Security Council in the same way that Resolution 2178 identified INTERPOL as the "global law enforcement information sharing" platform against foreign fighters.[231]

IV. CONCLUSION

Returning to the hypothetical introduced at the beginning of this Article, the foreign terrorists in that scenario might have been detected much earlier if the airlines had a "duty to report crime" (i.e. bottom-up vertical cooperation) and had access to the SLTD database (i.e. top-down vertical cooperation) managed by INTERPOL. Even if there were no immigration officers controlling the borders, as is the case with many global-digital crimes, which freely trespass state boundaries, the airline would have played its role as a frontline law enforcement officer.

Is it justifiable to shift such an obligation originally imposed on a government to the private sector? Answering this question can only be done by applying the complicated balancing test of culpability, as explained in my previous Article.

However, given that the modus operandi of some crimes discussed above is set within a globalized and digitalized context, there is a stronger rationale for imposing such a duty on the private sector. The modern context of crime often renders the traditional institutions and government actors (e.g. border control officers) employed by the government for crime detection somewhat powerless as the criminals abuse the networked space controlled by the private sector. Recall that in the hypothetical, the funds for terrorist activities were transferred to Paris through a financial network without any inspection by the border control officers. Only the financial institutions as choke point private actors could have detected it.

For the proposed "duty to report crime" regulations to be effective,

229. *See* Interpol I-Checkit Solution, *supra* note 14.
230. *See* UNNDPS, *supra* note 18, art. 1.
231. *See* S.C. Res. 2178, ¶ 18 (Sept. 24, 2014)

particularly those related to global-digital crime, high degrees of coordination along two dimensions are necessary. First, without global coordination between states, the domestic effort of imposing such a reporting duty on the private sector would be futile in detecting global-digital crime, which can easily displace itself to legal-loophole states. Thus, it is essential to establish global regulation of a "duty to report crime." Second, mutual coordination between government and choke point private actors is crucial to preventing information-loopholes. Since choke point private actors' "duty to report crime" currently consists of one-way bottom-up cooperation, global regulation of a "duty to report crime" should involve the responsibility of the government—namely, top-down cooperation of providing governmental crime information to choke point private actors—to shift the burden to the choke point private actors to work as frontline officers instead of government authorities.

In most domestic jurisdictions, including France, financial institutions (unlike airlines) are required to report suspicious activities. The terrorists in our hypothetical must have therefore used stolen passports to evade detection by the financial institutions by hiding their identity as known terrorists. If the information on the SLTD database had been shared with financial institutions, these hypothetical terrorist acts could have been detected and deterred at the initial stage of the terrorist plot. Although France was not a legal-loophole jurisdiction, the financial institution in France was an information-loophole abused by the terrorists.

This Article illustrates the international instantaneous sharing regime as an ideal regime for the global regulation of a "duty to report crime" to meet the above conditions. In addition, it suggests three criteria—horizontal accountability, vertical accountability, and proportionality to privacy/reputational harm—each of which is to be met, depending on the types of governmental information shared with choke point private actors by employing proper institutional and procedural manners.

As contemporary global regulations of a "duty to report crime" do not provide their own regimes of governmental information sharing with choke point private actors, the possible precedents comprising the current architecture of governmental crime information sharing with choke point private actors at the international level have been analyzed from the perspective of the three criteria. Each of these precedents is optimized to satisfy at least one, but not all three, criteria, except for information channel 2 in Chart I.

If global regulation of a "duty to report crime" is to have a one-size-fits-all regime for international, instantaneous sharing that will encompass all types of information, the regime should satisfy all three criteria. Thus, the proposed regime would match information channel 2 in Chart I,

wherein a global regulatory body would be established with two essential functions: first, it would work as an international data center to consolidate the governmental crime information and grant choke point private actors direct access; and second, it would act as a supervisory body to review the substance of the shared information and procedures of information production with the authority to penalize noncompliance. Under this unified structure, a global regulatory body would implement detailed processes and technical solutions to allow choke point private actors to access the database in the least intrusive manner.

So, is this just a pipedream?

Although it is in its embryonic stage, this proposal is more than just a pipedream. INTERPOL's I-Checkit program, adopted in 2015, enables participating airlines to directly query the SLTD whose information has been collected from participating member states. I-Checkit is the first and only regime to follow this channel 2 information flow in Chart I. Although INTERPOL does not play a supervisory role in the sense that it does not hold states accountable for providing false information through regular inspections and penalization, it nevertheless demonstrates the practicability of channel 2 in Chart I as a way of sharing international governmental information with choke point private actors. Considering that I-Checkit allows airlines, who have no duty to report terrorist activities, to directly access the SLTD, sharing of such international governmental information with choke point private actors, governed by global regulation of a "duty to report crime," is already strongly justified and, in the near future, should be firmly established.