# Part Two: Analyzing the Current Philippine Legal Framework and the Provisions of the Mutual Legal Assistance Treaties on Criminal Matters (MLATs) Entered by the Philippines in Relation to Transnational or Remote Cyber Searches and Seizures

*John Stephen B. Pangilinan*[★]



★ '20 J.D. *with honors*, Ateneo de Manila University School of Law. He was a Member of the *Ateneo Law Journal*'s Board of Editors. He was an Associate Lead Editor of the 3d issue of the *Journal*'s 62d Volume and Lead Editor of the 1st issue of *Journal*'s 64th Volume. He was also an editor of TENDING LIFE, a drug policy and anti-death penalty publication by the Anti-Death Penalty Task Force. He served as a volunteer legal intern for the Legal Interventions Department of International Justice Mission's (IJM) Pampanga Field Office and an intern for IJM's National Prosecution Development. He is also a research assistant at the Fr. Joaquin G. Bernas, S.J. Institute for Continuing Legal Education and Research at the Ateneo de Manila University School of Law. He previously wrote *Online Sexual Exploitation of Children: Applicable Laws, Casework Perspectives, and Recommendations*, 63 ATENEO L.J. 185 (2018); *Gender-Based Analysis of Laws Applicable to Child Sexual Exploitation Cases*, 63 ATENEO L.J. 355 (2018), both co-authored with Atty. Benjamin Lawrence Patrick E. Aritao; *Child Pornography and the Fictional and Non-Fictional Portrayal of Child Sexual Abuse*, 63 ATENEO L.J. 925 (2019); & *Comparative Study on Voluntary Arbitration and Commercial Arbitration, and Critique of the Supreme Court Decision in Fruehauf Electronics Philippines Corporation v. Technology Electronics Assembly and Management Pacific Corporation in Regard to Voluntary Arbitration*, 64 ATENEO L.J. 897 (2019).

This is the second part of the Author's Juris Doctor thesis titled "*Analyzing the No-Standing (to Question the Admissibility of Evidence Obtained and Impede the Execution of Requests) Provisions of the Mutual Legal Assistance Treaties on Criminal Matters (MLATs) Entered by the Philippines and the Implications of the MLATs on the Retrieved Evidence Relating to Transnational Cybercrimes*." The first part is published in the first Issue of this Volume.

*Cite as* 65 ATENEO L.J. 893 (2020).

## I. THE CROSSBREEDING DILEMMA

This Chapter begins with the explanation on the character of transnational crimes, which State should exercise jurisdiction over the same, and how can another State assist the other State who exercises jurisdiction over the crime. Thereafter, cybercrimes are defined, and it is explained how they were treated by the Philippines and other States. Finally, this Chapter concludes with defining transnational cybercrimes and explaining the States' treatment towards them.

*A. Transnational Crimes*

There is no concrete definition of transnational crimes. For example, the Oxford Bibliographies defines transnational crimes as "violations of law that involve more than one country in their planning, execution, or impact."[1] On the other hand, the United Nations Convention Against Transnational Organized Crime (UNCTOC) provides the circumstances that qualify an offense into a transnational crime, to wit:

(1) It is committed in more than one State;

(2) It is committed in one State but a substantial part of its preparation, planning, direction, or control takes place in another State;

(3) It is committed in one State but involves an organized criminal group that engages in criminal activities in more than one State; or

(4) It is committed in one State but has substantial effects in another State.[2]

The problem is that the definition does not identify whether the crime is punished by at least two or all States where any of the acts mentioned. For example, if a Filipino in the Philippines created a child pornographic fictional material (the act is punished in the Philippines) then he published the material in the United States (U.S.) (where the act is not considered a crime), is it considered a transnational crime? By inference, it should still be considered a transnational crime.

Neil Boister, a luminary in transnational criminal law, opined that transnational criminal law is part of international criminal law in a broad sense.[3] However, transnational crimes are strictly different from international crimes as the former involve the prosecution on a national level, whereas the latter involve the prosecution by the international community via the International Criminal Court, without regard to the characterization of the offense on a national level.[4]

1. Jay S. Albanese, Transnational Crime, *available at* http://www.oxfordbibliographies.com/view/document/obo-9780195396607/obo-9780195396607-0024.xml# (last accessed Nov. 30, 2020).

2. United Nations Convention Against Transnational Organized Crime and the Protocols Thereto art. 3 (2), *ratified* May 28, 2002, 2225 U.N.T.S. 209 [hereinafter UNCTOC].

3. NEIL BOISTER, AN INTRODUCTION TO TRANSNATIONAL CRIMINAL LAW 29 (1st ed. 2012).

4. *Id.* (citing R Cryer, *The Doctrinal Foundations of International Criminalization*, *in* INTERNATIONAL CRIMINAL LAW: SOURCES, SUBJECTS AND CONTENTS 125-26

Traditionally speaking, transnational crimes are separate and distinct from international crimes because transnational crimes do not arise from treaties, but recent developments show that there are transnational crimes that may also be defined and provided for by treaties.[5] A transnational crime is characterized as one that can be committed in a private capacity and against a private individual whereas international crime is one that is committed against the human race in general.[6] With this, a transnational crime may evolve to obtain a character of an international crime when it threatens "international peace and security or shock the conscience of mankind[.]"[7]

*B. Cybercrimes*

A cybercrime has no statutory definition in the Philippines despite the fact that it has already enacted the Cybercrime Prevention Act of 2012.[8] It only provides the acts that it punishes.[9]

The law classifies several acts into five groups:

(1) Offenses against the confidentiality, integrity, and availability of computer data and systems,[10]

(2) Computer-related offenses,[11]

(3) Content-related offenses,[12]

(4) Stage-based and participation-based offenses,[13] and

(MC Bassiouni, ed. 2008) & Rome Statute of the International Criminal Court, *ratified* Aug. 30, 2011, 2187 U.N.T.S. 3 [hereinafter Rome Statute]).

5. *See* BOISTER, *supra* note 3, at 19 (citing M.C. Boussiouni, *The Sources and Content of International Criminal Law: A Theoretical Framework*, *in* INTERNATIONAL CRIMINAL LAW 46 (M.C. Boussiouni, ed. 1998)).

6. BOISTER, *supra* note 3, at 18 & 19 (citing Rome Statute, *supra* note 4, art. 5).

7. BOISTER, *supra* note 3, at 19 (citing Cryer, *supra* note 4).

8. *See generally* An Act Defining Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes [Cybercrime Prevention Act of 2012], Republic Act No. 10175 (2012).

9. *Id.* §§ 4-6.

10. *Id.* § 4 (a).

11. *Id.* § 4 (b).

12. *Id.* § 4 (c).

13. *Id.* § 5 (b).

(5) Offenses under the Revised Penal Code and Special Penal Laws committed through a computer system.[14]

However, there is an overarching classification among these, specifically: (1) cyber-specific crimes and (2) modal cybercrimes. The first classification pertains to those that can only be committed through the use of the cyberspace (e.g., computer-related theft; this classification covers offenses against the confidentiality, integrity, and availability of computer data and systems and computer-related offenses).[15] On the other hand, modal cybercrimes pertain to those acts that were punished under the Cybercrime Prevention Act of 2012[16] on the basis of the mode over which they were committed. In other words, a person may also be punished for an act even when he or she did not use a computer system (e.g., a person who sells another for sex along the streets should be punished under the Anti-Trafficking in Persons Act of 2003, as amended,[17] but if he or she uses a computer system to do the act, he or she may be held liable for cybersex under the Cybercrime Prevention Act of 2012).[18] The provision of the law supports this proposition (e.g., Section 4, Subsection c, Paragraph 2 of the law provides that when an act under the Anti-Child Pornography Act of 2009[19] is committed *through* a computer system, it is considered a cybercrime.[20]).

Neither does the Budapest Convention, a multilateral treaty signed and ratified by the Philippines in 2017 and concurred in by Senate in 2018,[21]

14. Cybercrime Prevention Act of 2012, § 6.

15. *See id.* §§ 4-6.

16. *Id.*

17. An Act to Institute Policies to Eliminate Trafficking in Persons Especially Women and Children, Establishing the Necessary Institutional Mechanisms for the Protection and Support of Trafficked Persons, Providing Penalties for its Violations and for Other Purposes [Anti-Trafficking of Persons Act of 2003], Republic Act No. 9208 (as amended).

18. Cybercrime Prevention Act of 2012, § 4 (c) (1).

19. An Act Defining the Crime of Child Pornography, Prescribing Penalties Therefor and for Other Purposes [Anti-Child Pornography Act of 2009], Republic Act No. 9775 (2009).

20. Cybercrime Prevention Act of 2012, § 4 (c) (2) (emphasis supplied).

21. Senate of the Philippines, Senate Concurs in Ratification of Cybercrime Convention, Agreement Establishing AMRO, and Double Taxation Avoidance Treaties, *available at* http://www.senate.gov.ph/press_release/2018/0219_legarda1.asp (last accessed Nov. 30, 2020).

provide for the definition of a cybercrime.[22] Just like the Cybercrime Prevention Act of 2012,[23] the Budapest Convention only provides the acts that would constitute as a cybercrime.[24] These acts are classified into three: (1) access offenses,[25] (2) use offenses,[26] and (3) content offenses.[27]

The omission of the laws to exactly define cybercrime does not mean that they do not provide for its scope. If one looks at the punishable acts under the Cybercrime Prevention Act of 2012[28] and the Budapest Convention, one could conclude that the common denominator of these offenses is their mode of commission (i.e., through the use of a computer system).[29]

*C. Transnational Cybercrimes*

With the foregoing definitions and premises, it can be said that transnational cybercrime is an offense that is committed using a computer system, and is committed (1) "[i]n more than one State[,]"[30] (2) "[i]n one State but a substantial part of its preparation, planning, direction, or control takes place in another State[,]"[31] (3) "[i]n one State but involves an organized criminal group that engages in criminal activities in more than one State[,]"[32] or (4) "[i]n one

22. *See generally* Convention on Cybercrime ch. II, § 1, *opened for signature* Nov. 23, 2001, ETS No. 185, [hereinafter Budapest Convention].

23. *See generally* Cybercrime Prevention Act of 2012.

24. *See* Budapest Convention, *supra* note 22, ch. II, § 1, arts. 2-11.

25. Access offenses are those committed "against the confidentiality, integrity[,] and availability of computer data and systems." BOISTER, *supra* note 3, at 116 (citing Budapest Convention, *supra* note 22, art. 2).

26. Use offenses are those established crimes, e.g., forgery, committed through computers. BOISTER, *supra* note 3, at 117 (citing Budapest Convention, *supra* note 22, arts. 7 & 8). This Author characterizes these offenses as "modal cybercrimes."

27. Content offenses are those that are prohibited and punished because of the content generated, stored, transmitted, etc., through a computer system. BOISTER, *supra* note 3, at 117 (citing Budapest Convention, *supra* note 22, arts. 9-13).

28. *See generally* Cybercrime Prevention Act of 2012.

29. *See id.* §§ 4-6. *See also* Budapest Convention, *supra* note 22, ch. II, § 1, arts. 2-11.

30. UNCTOC, *supra* note 2, art. 3 (2) (a).

31. *Id.* art. 3 (2) (b).

32. *Id.* art. 3 (2) (c).

State but has substantial effects in another State." [33] Hence, the characterizations on transnational crimes and cybercrimes squarely apply to transnational cybercrimes since the transnational cybercrimes are a cross of the two classes of crimes.

## II. TERRITORIALITY IN THE CONTEXT OF CYBERCRIMES

Since it has been established that persons may question the admissibility of the evidence obtained via the Mutual Legal Assistance Treaties on Criminal Matters (MLAT), this Note proceeds with answering the question of which law will govern in examining the evidence obtained in transnational law enforcement against cybercrimes.

This Chapter discusses the right of States to exercise both judicial and law enforcement jurisdiction over crimes committed in the cyberspace. The analyses here are based on the view of territoriality since transnational cybercrimes occur in at least two or more States. The character of the cyberspace will first be discussed then the approaches exercised by States with regard to the territoriality in cyberspace (i.e., answering the question where a cybercrime takes place).

While it is clear in the Budapest Convention that a State-Party may exercise jurisdiction on cybercrime offenses committed within its territory[34] and the Rule on Cybercrime Warrants made it clear that Philippine Courts may exercise jurisdiction over a cybercrime if any of the elements of the offense occurred in the Philippines,[35] the definition of territory in terms of cyberspace is not clear.

Cyberspace is a complicated platform that a simple internet activity in a State may be accessible by a person in another State.[36] To illustrate, it works as if persons of different nations are placed in a single room — putting all

33. *Id*. art. 3 (2) (d).

34. Budapest Convention, *supra* note 22, art. 22 (1). *See also* Susan W. Brenner & Bert-Jaap Koops, *Approaches to Cybercrime Jurisdiction*, 4 J. HIGH TECH. L. 1, 10 (2004).

35. RULE ON CYBERCRIME WARRANTS, A.M. No. 17-11-03-SC, § 2.1 (August 15, 2018). *See also* Cybercrime Prevention Act of 2012, § 21.

36. Uta Kohl, *Jurisdiction in Cyberspace*, *in* RESEARCH HANDBOOK ON INTERNATIONAL LAW AND CYBERSPACE 37-38 (Nicholas Tsagourias & Russell Buchan eds., 2015) (citing David R. Johnson & David G. Post, *Law and borders —The rise of law in cyberspace*, 48 STAN. L. REV. 1367, 1399 (1996)).

persons who have access to the internet in a borderless dimension unique to the physical dimension where borders can be drawn.

States have adopted different approaches in determining whether the crime occurred in their territories to justify their exercise of jurisdiction over cybercrimes (i.e., accessibility, targeting, customary international law, and origin approach).[37]

*A. Accessibility*

The accessibility approach falls under the class of "destination approach."[38] Accessibility approach means that a State can exercise jurisdiction over transnational cybercrimes (mostly those that are content-based) if the act can be accessed by a person in the State.[39]

The most popular case that applied the approach is the *Licra and UEJF v. Yahoo! Inc. and Yahoo France*.[40] The case involves Yahoo!'s auctioning services via geocities.com; geocities.com may be accessed by persons in France via Yahoo.fr, which redirects a user to Yahoo.com.[41] Among the objects auctioned in geocities.com are Nazi objects, which are prohibited to be sold

37. *See generally* Kohl, *supra* note 36, at 37-51.

38. *See generally* Kohl, *supra* note 36, at 38. Destination approach or Country-of-Destination Approach means that a State can exercise jurisdiction over a cybercrime when a content or cybercrime can be downloaded in that State. *See also* Micheál Aaron O' Flynn, Harmonisation and Cybercrime Jurisdiction: Uneasy Bedfellows (An analysis of the jurisdictional trajectories of the Council of Europe's Cybercrime Convention), at 137 (2014) (unpublished Ph.D. dissertation, Queen Mary University of London) (on file with Queen Mary, University of London Library) (citing R v. Smith (Wallace Duncan), 4 QB 1418 (2004) (U.K.)).

39. *See* Kohl, *supra* note 36, at 38 (citing LICRA v. Yahoo! Inc., May 22, 2000 (Tribunal de Grande Instance de Paris), *available at* http://www.lapres.net/yahen.html (last accessed Nov. 30, 2020) (Fr.) [hereinafter *LICRA v. Yahoo! Inc.*]; LICRA & UEJF v. Yahoo! Inc. & Yahoo France, Nov. 20, 2000 (Tribunal de Grande Instance de Paris), *available at* http://www.lapres.net/yahen11.html (last accessed Nov. 30, 2020) (Fr.); & R v. Somm, Nov. 17, 1999 (Amtsgericht München) (Ger.)).

40. LICRA and UEJF v. Yahoo! Inc. and Yahoo France, May 22, 2000 (Tribunal de Grande Instance de Paris), *available at* http://www.lapres.net/yahen11.html (last accessed Nov. 30, 2020) (Fr.).

41. *LICRA v. Yahoo! Inc.*, whereas cl., para. 1 (this is a translated version of the French decision).

under French law.[42] The Tribunal de Grande Instance de Paris found Yahoo! liable for damages and ordered the injunction of the visualization of the Nazi objects in France.[43]

The bone of contention is whether French courts could exercise jurisdiction over the acts of selling Nazi objects via the internet where the seller is in the U.S. and a person in France could incidentally access the page.[44] The Tribunal ruled in the positive, saying that by "permitting the visualization in France of these objects and eventual participation of a surfer established in France in such an exposition [or] sale, Yahoo! Inc. thus has committed a wrong on the territory of France[.]"[45] Despite the argument of Yahoo! that it is "technically impossible to control access to its auction service or any other service, and that therefore it cannot prohibit any surfer from France from visualizing [the] same on his [or her] screen"[46] and that it has "warn[ed] all visitors against any uses of [its] services for purposes that are 'worthy of reprobation for whatsoever reason[,]'"[47] the Tribunal said that Yahoo!

> is in a position to identify the geographical origin of the site which is coming to visit, based on the IP address of the caller, which should therefore enable it to prohibit surfers from France, by whatever means are appropriate, from accessing the services and sites the visualization of which on a screen set up in France, and in some cases teledischarging and reproduction of the contents, or of any other initiative justified by the nature of the site consulted[.][48]

In other words, the Tribunal said that as long as the web host is capable of knowing and prohibiting the access of an act in another State where the act is illegal, the latter State may exercise jurisdiction over the act it considers illegal because the act is deemed to have taken place within its borders.[49]

---

42. *Id.* whereas cl., paras. 1–2 (citing Code de Procédure Pénale [CRIM. CODE], art. 645-2 (1804) (as amended) (Fr.)).

43. *LICRA v. Yahoo! Inc.*, *fallo*, paras. 3–4.

44. *Id.*

45. *Id.* whereas cl., para. 3.

46. *Id.* whereas cl., para. 5.

47. *Id.* whereas cl., para. 6.

48. *Id.* whereas cl., para. 7.

49. *LICRA v. Yahoo! Inc. See also* R v. Töben BGH, 1 StR 184/00 (2000) (Ger.) (where an Australian-hosted website was held liable under German law for holocaust-denying paraphernalia). In the *Töben* case, the German Court exercised jurisdiction because the content of the website, which was hosted in Australia, is

In sum, the accessibility approach can be applied in this example: if X is in Japan and produced an animated pornographic work of a child or *hentai* in a Japanese website and Y, a Filipino in the Philippines, accessed the porn produced by X by browsing in the Japanese server of the website, the Philippines may exercise jurisdiction over X for committing the act of producing fictional child pornography on the basis of accessibility because the crime is considered to have been committed in the Philippines.

*B. Targeting*

The targeting approach or theory states that a State may exercise territorial jurisdiction over a cybercrime if the act alleged to be a cybercrime is intended to have effect to the State.[50] Uta Kohl, a law professor and a writer on internet governance issues with particular focus on international dimensions and jurisdictions,[51] characterized the targeting approach as a moderate version of the destination approach, specifically, "not every State where a site can be accessed has the right to regulate it but only those States that are specifically targeted by [the site]."[52]

One of the famous cases that explains the targeting theory is *L'Oréal SA v. eBay International AG*.[53] L'Oréal filed a complaint against eBay for allowing persons who allegedly violated L'Oréal's intellectual property rights to transact in eBay's European websites.[54] L'Oréal alleged that when a person searches the term "shu uemura" in www.ebay.co.uk, the person will be directed to a list of products purporting to be shu uemura that originated from Hong Kong.[55] The issue now is whether courts in the United Kingdom (U.K.) could exercise jurisdiction over eBay, which is in another State, for allowing the sale

closely connected with Germany. *See* Kohl, *supra* note 36, at 39 (citing *Töben*, 1 StR 184/00).

50. *See* O' Flynn, *supra* note 38, at 137 (citing *Smith (Wallace Duncan)*, 4 QB 1418 (2004)) (U.K.). *See also* Kohl, *supra* note 36, at 45.

51. University of Southampton, Professor Uta Kohl BA/LLB (Hons) (University of Tasmania), Diploma in Legal Practice (ANU), PhD (University of Canberra), *available at* https://www.southampton.ac.uk/law/about/staff/uk1e18.page (last accessed Nov. 30, 2020).

52. Kohl, *supra* note 36, at 45.

53. L'Oréal SA v. eBay International AG, Judgment, Case C-324/09, ECLI:EU:C:2011:474 (CJEU July 12, 2011).

54. *Id.* ¶¶ 32-33.

55. *Id.* ¶¶ 39-41.

of counterfeit L'Oréal products.[56] The European Court of Justice ruled that "European trademark owners may prevent the sale, offer for sale[,] or advertising of goods located in a third State bearing their trademarks[.]"[57] Further, the Court clarified that "the mere fact that a website is accessible from the territory covered by the trade mark is not a sufficient basis for concluding that the offers for sale displayed there are targeted at consumers in that territory."[58]

Another case that illustrates the targeting approach is *Google Spain SL v. Agencia Española de Protección de Datos (AEPD)*.[59] This case involves the complaint filed by Costeja González against *La Vanguardia Ediciones* SL, Google Spain, and Google for the alleged unauthorized disclosure of his personal data relating to the attachment of his real estate properties for the recovery of his social security debts.[60] González alleged that when a person, outside Spain, who is browsing on Google in its general web server, i.e., the one not in Spain, González's name, the person will be given two links to the *La Vanguardia Ediciones* SL articles which allegedly disclose his personal data.[61] González sought to have the articles removed from Google's results page because the attachment proceedings had long been terminated.[62] The Agencia Española de Protección de Datos (AEPD) dismissed the case against *La Vanguardia Ediciones* SL but maintained the case against Google Spain and Google because Google is "subject to data protection legislation given that they carry out data processing for which they are responsible and act as intermediaries in the information society."[63] In affirming the position of the AEPD and the Audiencia Nacional of Spain, the European Court of Justice said that Google, Inc. may be held liable for the disclosure of personal data if "the operator of a search engine [i.e., Google in this case] sets up in a Member State [to the European Union] a branch or subsidiary which is intended to

56. *Id*. ¶ 50 (7).

57. Kohl, *supra* note 36, at 45 (citing *L'Oréal SA*, ECLI:EU:C:2011:474, ¶¶ 64 & 67).

58. Kohl, *supra* note 36, at 45 (citing *L'Oréal SA*, ECLI:EU:C:2011:474, ¶ 64).

59. Google Spain SL v. Agencia Española de Protección de Datos (AEPD), Judgment, Case C-131/12, ECLI:EU:C:2014:317 (CJEU May 13, 2014).

60. *Id*. ¶ 14.

61. *Id*. Basically, when a person "googles" Costeja González, the results would show the articles that allegedly disclose his personal data regarding the attachment of his properties. *Id*.

62. *Id*. ¶ 15.

63. *Id*. ¶ 17.

promote and sell advertising space offered by that engine and which orientates its activity towards the inhabitants of that Member State."[64]

*C. Customary International Law*

In customary international law, the rule that a State may exercise jurisdiction on acts that occurred outside its territory if the acts caused injuries within the State is found in the *Lotus*[65] and *Trail Smelter*[66] Cases. This rule is otherwise known as the effects doctrine, wherein a State may exercise jurisdiction over acts that although not occurring within its territories, would nevertheless have a negative effect to its territory.[67] In the context of cybercrimes, Uta Kohl, citing the Third Restatement of Foreign Relations Law, said that in order for a State to exercise jurisdiction on the basis of the effects doctrine, the exercise thereof must be reasonable, i.e.,

> the extent to which the activity has a substantial, direct[,] or foreseeable effect upon the territory, the character of the activity, the degree to which the desirability of regulation is generally accepted, the existence of justified expectations, the importance of regulating the activity, the consistency of the regulation with traditions of the international systems, the interest of other States in regulating the activity[,] and the likelihood of conflicting regulations.[68]

*D. Origin Approach*

Finally, the origin approach pertains to the theory that cybercrimes should only be prosecuted in the State where the activity was hosted.[69]

In a practical perspective, the origin approach affords a forewarning to the accused because he or she is presumably knowledgeable in the regulatory mechanisms of the State where he or she is doing the cybercrime.[70]

---

64. *Google Spain SL*, ECLI:EU:C:2014:317, ¶ 60.

65. SS Lotus (Fr. v. Turk.), Judgment, 1927 P.C.I.J. (ser. A) No. 10 (Sept. 7).

66. Award Relating to Trail Smelter Arbitration, 3 R.I.A.A. 1905 (1941).

67. Kohl, *supra* note 36, at 47.

68. *Id*. at 49 (citing RESTATEMENT (3D) OF FOREIGN RELATIONS LAW, § 403 (2) (1986)).

69. *See* Kohl, *supra* note 36, at 49 (citing Dow Jones & Co., Inc. v. Gutnick, HCA 56 (2002) (U.S.)).

70. *See* Kohl, *supra* note 36, at 49-50.

## III. CYBER SEARCHES AND SEIZURES

Since the jurisdictional questions on cybercrimes were already discussed in theoretical and practical perspectives in the preceding Chapter, the Author now proceeds to the enforcement mechanisms implemented by States, particularly the mechanism on searches and seizures.

As mentioned, this Note aims to discuss the usage of evidence obtained by a Foreign State against a person prosecuted in a Philippine Court vis-à-vis cybercrimes or a Philippine Law Enforcement Agent (LEA) abroad against a person prosecuted here. Hence, this Chapter discusses two aspects of cyber searches and seizures relevant to this Note (i.e., domestic, and international or transnational). The domestic approach discusses the fundamental doctrines on searches and seizures and the applications of the fundamental doctrines to cybercrimes. As regards the international or transnational approach, this Chapter discusses the general principles on transnational or transboundary law enforcement and some cases by foreign States and the criticisms thereto.

### *A. Domestic Approach to Cyber Searches and Seizures*

This Section discusses the Constitutional and jurisprudential principles governing searches and seizures in a Philippine perspective. It begins with the fundamental principles on searches and seizures then applies these fundamental principles to cybercrimes.

#### 1. Fundamental Principles

The Philippine Constitution provides the right of persons to privacy[71] and freedom from unreasonable searches and seizures.[72] With regard to both the rights to privacy and freedom from unreasonable searches and seizures, the Philippine Constitution provides that

> [t]he right of the people to be secure in their persons, houses, papers, and effects against unreasonable searches and seizures of whatever nature and for any purpose shall be inviolable, and no search warrant or warrant of arrest shall issue except upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized.[73]

71. PHIL. CONST. art. III, §§ 2 & 3 (1).

72. PHIL. CONST. art. III, § 2.

73. PHIL. CONST. art. III, § 2.

Another privacy right granted by the Constitution is the privacy of communication and correspondence to which the Constitution treats as inviolable and may only be intruded "upon lawful order of the court, or when public safety or order requires otherwise prescribed by law."[74]

This Part discusses the three general principles on searches and seizures, (i.e., search warrants, standing to question the search and seizure, and who may conduct the search and seizure).

*a. Search Warrants and Standing to Question Searches and Seizures*

As provided by the Constitution, a search warrant can only be issued "upon probable cause to be determined personally by the judge after examination under oath or affirmation of the complainant and the witnesses he may produce, and particularly describing the place to be searched and the persons or things to be seized."[75]

The case of *Aguilar v. Department of Justice*[76] describes probable cause as one which "exists when the facts are sufficient to engender a well-founded belief that a crime has been committed and that the respondent is probably guilty thereof."[77] The phrase "particularly describing the place to be searched and the persons or things to be seized"[78] does not refer to the exactitude of description but merely that the *descriptio personae* is sufficient for a law enforcer to identify the person to be arrested or place to be searched.[79] In terms of cybercrime, the Rule on Cybercrime Warrants has been adopted to tackle the requirement of particularity in a technical sense.[80]

For the purposes of questioning the validity of the search warrant or the search and seizure themselves, the person having the reasonable expectation of privacy over the thing seized or place searched may question the validity of the search or seizure.[81]

74. PHIL. CONST. art. III, § 3 (1).

75. PHIL. CONST. art. III, § 2.

76. Aguilar v. Department of Justice, G.R. No. 197522, 705 SCRA 629 (2013).

77. *Id.* at 639-40.

78. PHIL. CONST. art. III, § 2.

79. People v. Veloso, G.R. No. L-23051, 48 Phil. 169, 181 (1925).

80. *See* RULE ON CYBERCRIME WARRANTS, whereas cl., paras. 2 & 5.

81. *See* Stonehill v. Diokno, G.R. No. L-19550, 20 SCRA 383 (1967).

*b. State Agents*

In Constitutional law, the Bill of Rights is the security of persons against the State.[82] It cannot be invoked against the act of private individuals.[83] A State is not a physical entity; it does not have limbs to act on its own. Thus, it needs an agent or actor to pursue its interest.[84] But what constitutes a State agent? The following are the cases that defined — or rather described — a State agent.

i. *People v. Malngan*[85]

Edna Malngan was accused of Arson with Multiple Homicide.[86] From the facts culled by the Supreme Court from the lower courts' proceedings, Edna rode the pedicab of Rolando Gruta, a barangay *tanod*, 30 minutes prior to the discovery of the fire that burnt the house of Edna's employer.[87] The Barangay Chairman and his *tanods* received a report from Gruta that a woman, who happened to be Edna, was seen to have acted suspiciously and that the same woman rode his pedicab prior to the discovery of the fire.[88] Edna was brought to the Barangay Hall for investigation, where she thereafter confessed that she burnt the house of her employers in the presence of barangay officials and *tanods* and angry residents.[89] Upon her arraignment, she pleaded not guilty to the crime of Arson with Multiple Homicide.[90] During trial, the Barangay Chairman and the *tanod,* Gruta, were presented as witnesses.[91] This, among others, prompted her to file a demurrer to evidence saying that the testimonies of the witnesses against her are inadmissible as evidence.[92] The Regional Trial Court admitted her alleged confessions to the Barangay Chairman and *tanod*

82. People v. Marti, G.R. No. 81561, 193 SCRA 57, 67 (1991) (citing the Sponsorship Speech of Commissioner Bernas in the Record of the Constitutional Commission (1986)).

83. *Id.* at 64.

84. *See generally* Dela Cruz v. People, G.R. No. 209387, 779 SCRA 34 (2016).

85. People v. Malngan, G.R. No. 170470, 503 SCRA 294 (2006).

86. *Id.* at 302.

87. *Id.* at 300.

88. *Id.*

89. *Id.* at 300-01.

90. *Id.* at 302.

91. *Malngan*, 503 SCRA at 304-09.

92. *Id.* at 312.

as circumstantial evidence of her guilt.[93] The Court of Appeals affirmed the Regional Trial Court's decision.[94]

One of the issues presented before the Supreme Court is whether the confession made before the Barangay Chairman and *tanod* is admissible as evidence against Edna Malngan.[95] In excluding the testimonies of the *Barangay* Chairman and the *tanod* regarding her confession, the Court said —

> *Arguably*, the *barangay tanods*, including the *Barangay* Chairman, in this particular instance, *may* be deemed as [a] law enforcement officer for purposes of applying Article III, Section 12 (1) and (3), of the Constitution. When accused-appellant was brought to the *barangay* hall in the morning of 2 January 2001, she was already a suspect, actually the only one, in the fire that destroyed several houses as well as killed the whole family of Roberto Separa, Sr. She was, therefore, already under custodial investigation and the rights guaranteed by Article III, Section 12 (1), of the Constitution should have already been observed or applied to her. Accused-appellant's confession to *Barangay* Chairman Remigio Bernardo was made in response to the 'interrogation' made by the latter — admittedly conducted without first informing accused-appellant of her rights under the Constitution or done in the presence of counsel. For this reason, the confession of accused-appellant, given to Barangay Chairman Remigio Bernardo, as well as the lighter found by the latter in her bag are inadmissible in evidence against her as such were obtained in violation of her constitutional rights.[96]

While the Court categorized a Barangay Chairman and a barangay *tanod* as law enforcement agents (who are State actors) and the search and seizure they conducted to Edna as invalid, the Court did not provide a basis or standard to say that they were State actors.[97] This characterization was clarified in the next case.

ii. *People v. Lauga*

In *People v. Lauga*,[98] the Supreme Court characterized the *bantay bayan* as a law enforcement agent because it performs a function that is auxiliary to the

93. *Id.* at 313-14.

94. *Id.* at 314-15.

95. *Id.* at 315.

96. *Id.* at 324-25.

97. *See generally Malngan*, 503 SCRA.

98. People v. Lauga, G.R. No. 186228, 615 SCRA 548 (2010).

function of the Philippine National Police.[99] Furthermore, the Court explained that

> the specific scope of duties and responsibilities delegated to a '*bantay bayan*,' particularly on the authority to conduct a custodial investigation, any inquiry he [or she] makes *has the color of a state-related function and objective* insofar as the entitlement of a suspect to his [or her] constitutional rights provided for under Article III, Section 12 of the Constitution, otherwise known as the Miranda Rights, is concerned.[100]

With the above ruling, the Court has provided that the acts of a *bantay bayan* in the performance of his or her duties may be declared to violate the constitutional rights of a person because he or she, at the time of the performance of his or her duties as *bantay bayan*, "has the color of a state-related function and objective[.]"[101]

iii. *Dela Cruz v. People*

In *Dela Cruz v. People*,[102] the Supreme Court declared that a Port Personnel, although separate and distinct from a Port Police, is an "agent[ ] of [the] government under Article III of the Constitution"[103] because the functions that he or she performs "during routine security checks at ports have the color of a state-related function."[104]

Here, the Supreme Court expanded the doctrines in *Malngan* and *Lauga* to the entirety of Article III of the Philippine Constitution (i.e., for as long as a person performs functions that have the color of state-related function, his or her functions fall under the contemplation of Article III of the Constitution).[105]

99. *Id.* at 557 (citing People v. Buendia, G.R. Nos. 145318-19, 382 SCRA 471, 718 (2002)).

100. *Lauga*, 615 SCRA at 558 (emphasis supplied).

101. *Id.*

102. *Dela Cruz*, 779 SCRA.

103. *Id.* at 60.

104. *Id.* In the subsequent portions of the *ponencia*, the Supreme Court quoted *People v. Lauga* to find basis in holding that the functions of the port personnel have the color of a State-related function. *Id.* at 60-61 (citing *Lauga*, 615 SCRA at 558).

105. *Dela Cruz*, 779 SCRA at 60.

iv. *Miguel v. People*[106]

In this case, the Court affirmed its rulings in *Malngan,*[107] *Lauga,*[108] and *Dela Cruz*.[109] The Supreme Court emphasized that Article III of the Constitution can be invoked against a civilian volunteer or a private individual if he or she "*act*[ed] *under the color of a state-related function*."[110]

*c. Searches and Seizures by Persons who are not Agents of the State*

As mentioned by the cited jurisprudence above, the protections found in Article III of the Constitution can only be invoked against the State.[111] The protections there do not cover non-State actors or persons who are not acting on behalf of the Philippine Government.[112] The Supreme Court, in *People v. Marti*, said —

> The constitutional proscription against unlawful searches and seizures therefore applies as a restraint directed only against the government and its agencies tasked with the enforcement of the law. Thus, it could only be invoked against the State to whom the restraint against arbitrary and unreasonable exercise of power is imposed.[113]

The Court also reiterated the basic principle in Constitutional law that the limits provided by the Constitution are only applicable against the State and not to private individuals.[114] Furthermore, it was earlier declared by the Court that the Constitution is a social contract between the State — specifically, the Philippine State as represented by its Government — and the individuals wherein the latter "have surrendered their sovereign powers to the State for the common good[,]"[115] in addition to the allocation and limitation of State power.[116] Thus, the provisions of the Constitution regarding the rights of

106. Miguel v. People, G.R. No. 227038, 833 SCRA 440 (2017).

107. *Malngan*, 503 SCRA.

108. *Lauga*, 615 SCRA.

109. *Miguel*, 833 SCRA at 449-51 (citing *Dela Cruz*, 779 SCRA at 60-61).

110. *Miguel*, 833 SCRA at 449 (citing *Dela Cruz*, 779 SCRA at 60-61).

111. *See Dela Cruz*, 779 SCRA at 60.

112. *See Marti*, 193 SCRA at 67.

113. *Marti*, 193 SCRA at 67.

114. *Id.* at 68.

115. Marcos v. Manglapus, G.R. No. 88211, 177 SCRA 668, 693 (1989).

116. *Id.*

individuals are only enforceable against the acts of the Philippine government or its agents but not to private individuals.[117]

2. Cyber Searches and Seizures

This Part discusses how the Philippines treats cyber searches and seizures by looking to the parallel treatments and the treatments that are different from physical search and seizure. This also discusses the landmark cases on cybercrimes and cyber privacy and the Rule on Cybercrime Warrants.

*a. Cases on Cybercrimes and Cyber Privacy*

The *Disini, Jr. v. Secretary of Justice*[118] case tackled the Constitutional issues surrounding the Cybercrime Prevention Act of 2012.[119] Among those is the issue on the right to informational privacy of a person vis-à-vis his or her data stored in his or her computer which may have been linked to the internet.[120]

The Court first discussed the nature of the privacy right. To wit —

> In *Whalen v. Roe*, the [Supreme Court of the United States (SCOTUS)] classified privacy into two categories: decisional privacy and informational privacy. Decisional privacy involves the right to independence in making certain important decisions, while informational privacy refers to the interest in avoiding disclosure of personal matters. It is the latter right — the right to informational privacy — that those who oppose government collection or recording of traffic data in real-time seek to protect.
>
> Informational privacy has two aspects: the right not to have private information disclosed, and the right to live freely without surveillance and intrusion. In determining whether or not a matter is entitled to the right to privacy, this Court has laid down a two-fold test. The first is a subjective test, where one claiming the right must have an actual or legitimate expectation of privacy over a certain matter. The second is an objective test, where his or her expectation of privacy must be one society is prepared to accept as objectively reasonable.[121]

In discussing the privacy expectations of internet and other information and communication technology (ICT) users, the Court said —

117. *See Marti*, 193 SCRA at 67-68.

118. Disini, Jr. v. Secretary of Justice, G.R. No. 203335, 716 SCRA 237 (2014).

119. *See Disini, Jr.*, 716 SCRA at 299-300.

120. *Disini, Jr.*, 716 SCRA at 336-37.

121. *Id.* at 339-40 (citing Whalen v. Roe, 429 U.S. 589, 599 (1977) & Pollo v. Constantino-David, G.R. No. 181881, 659 SCRA 189, 206 (2011)).

> [A]n ordinary ICT user who courses his [or her] communication through a service provider, must of necessity disclose to the latter, a third person [(this is the Internet Service Provider)], the traffic data needed for connecting him to the recipient ICT user. For example, an ICT user who writes a text message intended for another ICT user must furnish his service provider with his [or her] cell phone number and the cell phone number of his [or her] recipient, accompanying the message sent. It is this information that creates the traffic data. *Transmitting communications is akin to putting a letter in an envelope properly addressed, sealing it closed, and sending it through the postal service. Those who post letters have no expectations that no one will read the information appearing outside the envelope.*
>
> Computer data — messages of all kinds — travel across the internet in packets and in a way that may be likened to parcels of letters or things that are sent through the posts. *When data is sent from any one source, the content is broken up into packets and around each of these packets is a wrapper or header.* This header contains the traffic data: information that tells computers where the packet originated, what kind of data is in the packet (SMS, voice call, video, internet chat messages, email, online browsing data, etc.), where the packet is going, and how the packet fits together with other packets. *The difference is that traffic data sent through the internet at times across the ocean do not disclose the actual names and addresses (residential or office) of the sender and the recipient, only their coded internet protocol (IP) addresses.* The packets travel from one computer system to another where their contents are pieced back together. Section 12 [of the Cybercrime Prevention Act of 2012] does not permit law enforcement authorities to look into the contents of the messages and uncover the identities of the sender and the recipient.
>
> For example, when one calls to speak to another through his [or her] cellphone, the service provider's communication's system will put his [or her] voice message into packets and send them to the other person's cellphone where they are refitted together and heard. The latter's spoken reply is sent to the caller in the same way. To be connected by the service provider, the sender reveals his cellphone number to the service provider when he puts his call through. He [or she] also reveals the cellphone number to the person he [or she] calls. The other ways of communicating electronically follow the same basic pattern.[122]

Furthermore, the *ponencia* held that

> when seemingly random bits of traffic data are gathered in bulk, pooled together, and analyzed, they reveal patterns of activities which can then be used to create profiles of the persons under surveillance. With enough traffic

122. *Disini, Jr.*, 716 SCRA at 340–41 (citing Jonathan Strickland, How IP Convergence Works, *available at* http://computer.howstuffworks.com/ip-convergence2.htm (last accessed Nov. 30, 2020)) (emphases supplied).

> data, analysts may be able to determine a person's close associations, religious views, political affiliations, even sexual preferences.[123]

Because of that reality, the Court said that an ICT user has a reasonable expectation of privacy over the data that he or she has sent.[124] The Court declared the provision of the Cybercrime Prevention Act of 2012 on real-time collection of data unconstitutional because of the unreasonable standard that it imposes to search the correspondences of ICT users over which they have a reasonable expectation of privacy.[125]

Additionally, Justice Antonio T. Carpio, in his separate opinion, reasoned that the invocation of *Smith v. Maryland*,[126] a U.S. case where the SCOTUS held that a telephone user has no reasonable expectation of privacy over his or her activities of dialing a particular telephone number,[127] is not meritorious because the "three modern Philippine Constitutions ... guarantee the 'privacy of communication and correspondence.'"[128] Justice Carpio further explained that

> [a]lthough such guarantee readily protects the *content* of private communication and correspondence, the guarantee also protects traffic data collected *in bulk* which enables the government to construct profiles of individuals' close social associations, personal activities and habits, political and religious interests, and lifestyle choices, enabling intrusion into their lives as extensively as if the government was physically searching their 'houses, papers[,] and effects.'[129]

Furthermore, Justice Carpio cited that there is already a radical change in the circumstances that warrant the review of *Smith*.[130] Finally, he mentioned

123. *Disini, Jr.*, 716 SCRA at 342 (citing *Disini, Jr.*, 716 SCRA at 450-72 (J. Carpio, concurring and dissenting opinion) & *Disini, Jr.*, 716 SCRA at 487-511 (J. Brion, separate concurring opinion)).

124. *Disini, Jr.*, 716 SCRA at 343-44.

125. *Id.*

126. Smith v. Maryland, 442 U.S. 735 (1979).

127. *Disini, Jr.*, 716 SCRA at 457 (J. Carpio, concurring and dissenting opinion) (citing *Smith*, 442 U.S. at 744).

128. *Disini, Jr.*, 716 SCRA at 457 (1935 PHIL. CONST. art. III, § 1 (5) (superseded 1973); 1973 PHIL. CONST. art. IV, § 4 (1) (superseded 1986); & PHIL. CONST. art. III, § 3 (1)).

129. *Disini, Jr.*, 716 SCRA at 458 (citing RULE ON HABEAS DATA, A.M. No. 08-1-16-SC (Feb. 2, 2008)).

130. *Disini, Jr.*, 716 SCRA at 459 (citing Klayman v. Obama, 957 F. Supp. 2d 1, 31 (D.D.C. 2013) (U.S.)).

that a user only discloses his or her information to a service provider out of necessity to avail the latter's services (i.e., he or she does not expect that the information disclosed be likewise disclosed to the government).[131]

In sum, a person who stores and transmits computer data may have a reasonable expectation of privacy over the data.[132] With this, the government cannot simply hack into his or her computer system without a search warrant to that effect.[133]

*b. The Rule on Cybercrime Warrants*

Due to the technical nature of cybercrimes and the cyberspace, the traditional modes of searches and seizures are not entirely applicable.[134] Hence, the Court adopted the Rule on Cybercrime Warrants.[135]

The Rule covers the "application and grant of warrants and related orders involving the preservation, disclosure, interception, search, seizure, and/or examination, as well as the custody, and destruction of computer data"[136] in relation to the violations of the Cybercrime Prevention Act of 2012.[137] In a cybercrime case, the Rule clarifies that the Rules on Criminal Procedure are still applicable, and the Rule on Cybercrime Warrants is only a supplement thereto.[138]

The Rule discusses four types of warrants vis-à-vis cybercrimes, namely:

(1) Warrant to Disclose Computer Data (WDCD);[139]

(2) Warrant to Intercept Computer Data (WICD);[140]

(3) Warrant to Search, Seize and Examine Computer Data (WSSECD);[141] and

131. *Disini, Jr.*, 716 SCRA at 459.

132. *Id.* at 460.

133. *Id.*

134. RULE ON CYBERCRIME WARRANTS, whereas cl., para. 2.

135. *Id.* whereas cl., para. 5.

136. *Id.* § 1.2.

137. *Id.*

138. *Id.* § 1.3.

139. *Id.* § 4.

140. RULE ON CYBERCRIME WARRANTS, § 5.

141. *Id.* § 6.

(4) Warrant to Examine Computer Data (WECD).[142]

WDCD is a Court order allowing an LEA to

> issue an order requiring any person or service provider to disclose or submit subscriber's information, traffic data[,] or relevant data in his[,] her[,] or its possession or control within [72] hours from receipt of the order in relation to a valid complaint officially docketed and assigned for investigation and the disclosure is necessary and relevant for the purpose of investigation.[143]

For WICD, the Rule provides for the definition of the term "interception," which "refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content data, either directly, through access and use of a computer system, or indirectly through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring."[144] According to the Rule, a WICD authorizes an LEA to conduct

> (a) listening [ ], (b) recording, (c) monitoring, or (d) surveillance of the content of communications, including procuring of the content of computer data, either directly, through access and use of a computer system or indirectly, through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring.[145]

A WSSECD, on the other hand, authorizes an LEA "to search the particular place for items to be seized and/or examined."[146] This search, seizure, and examination must be made to computer data.[147] This covers a situation where the LEAs do not have in their possession a computer system suspected to contain data in relation to cybercrime.[148] If the LEAs already have possession of a computer system (e.g., cellphone, laptop, desktop, computer tablet, video camera etc.), which is suspected to contain computer data in relation to the commission of a cybercrime, the LEAs should apply for a

142. *Id.* § 6.9.

143. *Id.* §§ 4.1 & 4.2.

144. *Id.* § 1.4 (k) (citing Cybercrime Prevention Act of 2012, § 3 (m) & Rules and Regulations Implementing Republic Act No. 10175, Otherwise Known as the "Cybercrime Prevention Act of 2012", Republic Act No. 10175, rule I, § 3 (aa) (2015)).

145. RULE ON CYBERCRIME WARRANTS, § 5.2.

146. *Id.* § 6.1.

147. *Id.* § 6.2.

148. *Id.*

WECD.[149] The Section on WECD specifically says that no examination of the contents of a computer device or system lawfully obtained shall be made without a WECD.[150] In other words, WSSECD is issued when LEAs do not have in their possession a device that contains a computer data whereas a WECD is issued when the LEAs already have possession of a device — the end goal of both is to search the computer data in the device.[151]

3. Section Summary

In fine, the following must be noted in cyber searches and seizures:

(1) The constitutional protections against unreasonable searches and seizures are applicable only to the acts of State agents;[152] and

(2) In cyber searches and seizures, a cybercrime warrant is necessary before any act of search and seizure can be done to a computer data.[153]

*B. Principles on Transnational or Transborder Law Enforcement*

This Section discusses the conflict of laws rules governing searches and seizures and general principles on transnational or transborder law enforcement. It begins with the discussion of the act of state doctrine. Then, the Section discusses the territoriality approach in light of a situation when the search is presumably made in the Philippines by a foreign State. Finally, it discusses the effect of the MLAT provisions on the governing law in the execution of requests in analyzing the validity of search and seizure done by a foreign State.

1. Act of State Doctrine

The act of state doctrine provides that local courts are precluded "from inquiring into the validity of the public acts a recognized foreign sovereign power committed within its own territory."[154] In other words, a court cannot look into the validity of an act of a foreign State if:

149. *Id.* § 6.9.

150. *Id.* § 6.9, para. 1.

151. *See* RULE ON CYBERCRIME WARRANTS, §§ 6.1, 6.2, & 6.9.

152. *See Dela Cruz*, 779 SCRA at 60.

153. *See* RULE ON CYBERCRIME WARRANTS, §§ 4.1, 4.2, 5, 5.2, 6, 6.1, 6.2, & 6.9.

154. Banco Nacional de Cuba v. Sabbatino, 376 U.S. 398, 401 (1964).

(1) The act is done in the foreign State's governmental capacity or *jure imperii*;[155] and

(2) The act is made within the foreign State's territory.[156]

This rule is not absolute. In the same case where the quoted definition was culled, the SCOTUS clarified that international law does not require the application of States of the said doctrine.[157] Furthermore, the SCOTUS said —

> The text of the [U.S.] Constitution does not require the act of state doctrine; it does not irrevocably remove from the judiciary the capacity to review the validity of foreign acts of state.
>
> The act of state doctrine does, however, have 'constitutional' underpinnings. It arises out of the basic relationships between branches of government in a system of separation of powers. It concerns the competency of dissimilar institutions to make and implement particular kinds of decisions in the area of international relations. The doctrine, as formulated in past decisions, expresses the strong sense of the Judicial Branch that its engagement in the task of passing on the validity of foreign acts of state may hinder, rather than further, this country's pursuit of goals both for itself and for the community of nations as a whole in the international sphere.[158]

Hence, the doctrine serves as a form of judicial restraint in order to avoid any prejudice to the foreign relations of a State with another State because a matter of foreign relations is principally lodged in the Executive — the remedy of a person injured by a foreign State's public act within its territory is to "exhaust local remedies and then repair to the executive authorities of his own state to persuade them to champion his [or her] claim in diplomacy or before an international tribunal."[159]

---

155. *Id.* Acts done in *jure imperii* must be distinguished from acts *jure gestionis*. The former involves those functions that relate to the governmental functions while the latter involves the commercial, private, and proprietary acts of a State. *See* Arigo v. Swift, G.R. No. 206510, 735 SCRA 102, 149 (2014) (C.J. Sereno, concurring opinion) (citing China Natural Machinery & Equipment Corp. v. Hon. Santamaria, G.R. No. 185572, 665 SCRA 189, 197 (2012)).

156. *Banco Nacional de Cuba*, 376 U.S. at 401.

157. *Id.* at 421-22 (citing LASSA F.L. OPPENHEIM, 1 OPPENHEIM'S INTERNATIONAL LAW, § 115aa (Lauterpacht, 8th ed. 1955)).

158. *Banco Nacional de Cuba*, 376 U.S. at 423.

159. Presidential Commission on Good Governance v. Sandiganbayan, G.R. No. 124772, 530 SCRA 13, 25-26 (2007) (citing *Banco Nacional de Cuba*, 376 U.S.).

2. Territoriality Integrity, Non-Interference, and Presumption Against Extraterritoriality

A State cannot exercise its sovereign power, such as arresting a person who violated its laws, in the territory of another State.[160] Doing so would violate its obligation under international law wherein States "shall refrain in their international relations from the threat or use of force against the territorial integrity or political independence of any [S]tate[.]"[161]

A State, without the permission of another State, cannot exercise its law enforcement jurisdiction in another State as it "would run headlong into the customary international law norm of territorial sovereignty."[162] In Philippine jurisprudence, for example, it is recognized that "[e]xtradition is an intrusion into the territorial integrity of the host State and a delimitation of the sovereign power of the State within its own territory."[163] Furthermore, a State which is a party to an extradition treaty is not obliged to surrender a person under an extradition request.[164] This characterization of the Philippine Supreme Court implies that when it comes to law enforcement, a sovereign State has supreme law enforcement power within its territory.[165]

One of the most talked about topics in transnational law enforcement is the questioning of the validity of arrests conducted by a State's law enforcers in another State. For example, Philippine LEAs went to Canada to arrest a person in Canada by kidnapping the latter with the consent of Canadian LEA. In situations similar to that example, the question whether to apply the doctrine of *male captus, bene detentus* arises. The doctrine of *male captus, bene*

160. Christian Marxsen, *Territorial Integrity in International Law — Its Concept and Implications for Crimea*, 75 ZAÖRV 7, 12-13 (2015) (citing J. DELBRÜCK & R. WOLFRUM, 1 VÖLKERRECHT 792-93 (2d ed., 2002)).

161. U.N. CHARTER, art. 2 (4). *See also* Marxsen, *supra* note 160, at 13.

162. Justin M. Sandberg, *The Need for Warrants Authorizing Foreign Intelligence Searches of American Citizens Abroad: A Call for Formalism*, 69 U. CHI. L. REV. 403, 426 (2002) (citing Ayaz R. Shaikh, *A Theoretic Approach to Transnational Terrorism*, 80 GEO. L.J. 2131, 2159 (1992)).

163. Wright v. Court of Appeals, 235 SCRA 341, 344 (1994) (citing LASSA F.L. OPPENHEIM, INTERNATIONAL LAW: A TREATISE 362-69 (1912)).

164. *Wright*, 235 SCRA at 344-45.

165. *See id.* at 344 (where the Supreme Court said "even with a treaty rendered executory upon ratification by appropriate authorities, does not impose an obligation to extradite on the requested State until the latter has made its own determination of the validity of the requesting State's demand, in accordance with the requested State's own interests").

*detentus* provides that an accused cannot question the validity of the arrest if the arrest was made outside the court's territorial jurisdiction.[166] In some cases, even the effects of the arrest, like the subsequent search, may not also be questioned under the doctrine.[167]

In the U.S. and Israel, that doctrine is being used by their respective courts.[168] However, countries like the U.K. and South Africa have refused to apply the doctrine because courts cannot accept the fact that a violation of international law and domestic law of another State cannot be used to pursue State's interest.[169]

Another aspect of respecting another State's sovereignty is the presumption against extraterritoriality (i.e., laws enacted by States are intended to apply only to the acts within its borders or acts that have effect in within its borders).[170]

3. MLAT Provisions

The MLATs entered by the Philippines contain provisions stating that in the execution of a search and seizure request, the law of the Requested State applies. Below is the enumeration of the MLATs with the corresponding provision:

| Treaty | Execution of Search and Seizure Provision |
|---|---|
| AUS-PH MLAT | "The Requested State shall insofar as its law permits carry out requests for search, seizure[,] and delivery of any material to the Requesting State |

166. Ronald Glenn T. Tuazon, *Wrongful Capture, Proper Detention? Challenging the Doctrine of Male Captus, Bene Detentus in International Law*, 56 ATENEO L.J. 37, 39-40 (2011) (citing ILLIAS BANTEKAS & SUSAN NASH, INTERNATIONAL CRIMINAL LAW 218 (2007)).

167. *See, e.g.*, Ker v. Illinois, 119 U.S. 436 (1886) & Frisbie v. Collins, 342 U.S. 519 (1952).

168. *See, e.g.*, U.S. v. Alvarez-Machain, 504 U.S. 655 (1992) & Attorney General v. Adolf Eichmann, 36 I.L.R. 277 (1962) (Isr.). *See also* Tuazon, *supra* note 166, at 40.

169. Tuazon, *supra* note 166, at 48-49 (citing Bennett v. Horseferry, 1 A.C. 42, 67 (1994) (U.K.) & State v. Ebrahim, 21 I.L.M. 888 (1991) (S.A.)).

170. William S. Dodge, *Understanding the Presumption Against Extraterritoriality*, 16 BERKELEY J. INT'L L. 85, 88 (1998). *See also* Kiobel v. Royal Dutch Petroleum Co., 569 U.S. 108 (2013).

| | |
|---|---|
| | provided the request contains information that would justify such action under the law of the Requested State."[171] |
| U.S.-PH MLAT | "The Requested State shall execute a request for the search, seizure, and delivery of any item to the Requesting State if the request includes the information justifying such action under the laws of the Requested State."[172] |
| China-PH MLAT | "The Requested Party shall, to the extent its national law permits, execute a request for inquiry, examination, search, freezing and seizure of evidential materials, articles and assets."[173] |
| HK-PH MLAT | "The Requested Party shall insofar as its law permits carry out requests for search[,] seizure[,] and delivery of any material to the Requesting Party provided the request contains information that would justify such action under the law of the Requested Party."[174] |

171. Treaty Between Australia and the Republic of the Philippines on Mutual Legal Assistance in Criminal Matters, Phil.-Aus., art. 17 (1), Apr. 28, 1988, 1770 U.N.T.S. 209 [hereinafter AUS-PH MLAT].

172. The Treaty Between the Government of the United States of America and the Government of the Republic of the Philippines on Mutual Legal Assistance in Criminal Matters, Phil.-U.S., art. 14 (1), Nov. 13, 1994, 1994 U.N.T.S. 309 [hereinafter U.S.-PH MLAT].

173. Treaty between the Republic of the Philippines and People's Republic of China concerning Mutual Legal Assistance on Criminal Matters, Phil.-China, art. 13 (1), Oct. 16, 2000 [hereinafter China-PH MLAT].

174. Agreement between the Government of the Hong Kong Special Administrative Region of the People's Republic of China and the Government of the Republic of the Philippines concerning mutual legal assistance in criminal matters, Phil.-H.K., art. XVII (1), Feb. 23, 2001, 2754 U.N.T.S. 145 [hereinafter HK-PH MLAT].

| | |
|---|---|
| Swiss-PH MLAT | "A request shall be executed in accordance with the law of the Requested State."[175] Any special request for procedure in the conduct of the search must be expressly stated in the request subject to the laws of the Requested State.[176] |
| PH-Korea MLAT | "The Requested Party shall, to the extent its laws permit, carry out requests made in respect of a criminal matter in the Requesting Party for the search, seizure[,] and delivery of material to that Party."[177] |
| PH-Spain MLAT | "The Requested State shall execute a request for the search, seizure, and delivery of any property to the Requesting State if the request includes the information justifying such action under the laws of the Requested State."[178] |
| UK-PH MLAT | "The Requested State shall carry out requests for search, seizure[,] and delivery of any evidence to the Requesting State provided the request contains information that would justify such action under the domestic law of the Requested State."[179] |

175. Treaty on Mutual Legal Assistance in Criminal Matters Between the Republic of the Philippines and the Swiss Confederation, Phil.-Switz., art. 4 (1), July 9, 2002 [hereinafter Swiss-PH MLAT].

176. *Id.* art. 4 (2).

177. Treaty between the Republic of the Korea and the Republic of the Philippines on mutual legal assistance in criminal matters, Phil.-S. Kor., art. 16 (1), June 3, 2003, Treaty No. 53251 [hereinafter PH-Korea MLAT].

178. Treaty on Mutual Legal Assistance in Criminal Matters the Republic of the Philippines and the Kingdom of Spain, Phil.-Spain, art. 16 (1), Mar. 2, 2004 [hereinafter PH-Spain MLAT].

179. Treaty on Mutual Legal Assistance in Criminal Matters between the United Kingdom of Great Britain and Northern Ireland and the Republic of the

| | |
|---|---|
| ASEAN MLAT | "The Requested Party shall, subject to its domestic laws, execute a request for the search, seizure[,] and delivery of any documents, records or items to the Requesting Party if there are reasonable grounds for believing that the documents, records or items are relevant to a criminal matter in the Requesting Party."[180] |
| Budapest Convention | "Mutual assistance requests under this article shall be executed in accordance with the procedures specified by the requesting Party, except where incompatible with the law of the requested Party."[181] |

With all the provisions cited above, the common denominator is that when a Requested State is asked to conduct search and seizure within its territory:

(1) The basis of the search and seizure in the Requested State must be based on its laws, e.g., in the Philippines, there must be a probable cause;[182] and

(2) The execution of the search and seizure must also be in accordance with the law of the Requested State.[183]

---

Philippines, Phil.-U.K., art. 16 (1), Sep. 18, 2009, Treaty No. 52700 [hereinafter UK-PH MLAT].

180. Treaty on Mutual Legal Assistance in Criminal Matters, art. 18 (1), *opened for signature* Jan. 17, 2006, ASEAN Treaty No. 195 [hereinafter ASEAN MLAT].

181. Budapest Convention, *supra* note 22, art. 27 (3).

182. *See* AUS-PH MLAT, *supra* note 171, art. 17 (1); U.S.-PH MLAT, *supra* note 172, art. 14 (1); China-PH MLAT, *supra* note 173, art. 13 (1); HK-PH MLAT, *supra* note 174, art. XVII (1); Swiss-PH MLAT, *supra* note 175, art. 4 (1)-(2); PH-Korea MLAT, *supra* note 177, art. 16 (1); PH-Spain MLAT, *supra* note 178, art. 16 (1); UK-PH MLAT, *supra* note 179, art. 16 (1); ASEAN MLAT, *supra* note 180, art. 18 (1); & Budapest Convention, *supra* note 22, art. 27 (3). *See also* PHIL. CONST. art III, § 2.

183. *See* AUS-PH MLAT, *supra* note 171, art. 17 (1); U.S.-PH MLAT, *supra* note 172, art. 14 (1); China-PH MLAT, *supra* note 173, art. 13 (1); HK-PH MLAT, *supra*

4. Section Summary

From the above, it can be said that in transnational law enforcement, the following applies:

(1) A local court cannot sit to decide the validity of a public act done by another State within its territory;[184]

(2) The laws of a State are presumably applicable only to those acts within its borders or those acts affecting its territory;[185]

(3) A State must respect the territorial integrity of another State;[186] and

(4) Whenever an MLA request is being executed by a foreign State within its territory, its laws govern.[187]

*C. Transnational or Remote Searches and Seizures*

This Section shows the treatment of other States with regard to searches and seizures done outside their territory by their own agents. This Section discusses the international cooperation provisions of the Cybercrime Prevention Act of 2012, its Implementing Rules and Regulations (IRR), and the Rule on Cybercrime Warrants, the notorious case of *U.S. v. Gorshkov*,[188] and criticisms thereto. The Section also shows how other States oppose the approach made in *Gorshkov* and how the learnings therefrom can be applied in the present case.

---

note 174, art. XVII (1); Swiss-PH MLAT, *supra* note 175, art. 4 (1)-(2); PH-Korea MLAT, *supra* note 177, art. 16 (1); PH-Spain MLAT, *supra* note 178, art. 16 (1); UK-PH MLAT, *supra* note 179, art. 16 (1); ASEAN MLAT, *supra* note 180, art. 18 (1); & Budapest Convention, *supra* note 22, art. 27 (3).

184. *Banco Nacional de Cuba*, 376 U.S. at 401.

185. Dodge, *supra* note 170, at 88 & *Kiobel*, 569 U.S.

186. U.N. CHARTER, art. 2, ¶ 4.

187. *See* AUS-PH MLAT, *supra* note 171, art. 17 (1); U.S.-PH MLAT, *supra* note 172, art. 14 (1); China-PH MLAT, *supra* note 173, art. 13 (1); HK-PH MLAT, *supra* note 174, art. XVII (1); Swiss-PH MLAT, *supra* note 175, art. 4 (1)-(2); PH-Korea MLAT, *supra* note 177, art. 16 (1); PH-Spain MLAT, *supra* note 178, art. 16 (1); UK-PH MLAT, *supra* note 179, art. 16 (1); ASEAN MLAT, *supra* note 180, art. 18 (1); & Budapest Convention, *supra* note 22, art. 27 (3).

188. U.S. v. Gorshkov, 2001 WL 1024026 (2001) (U.S.).

1. Cybercrime Prevention Act of 2012, its Implementing Rules and Regulations (IRR), and the Rule on Cybercrime Warrants

The Cybercrime Prevention Act of 2012 allows international cooperation in relation to the "investigations or proceedings concerning criminal offenses related to computer systems and data, or [to] the collection of evidence in electronic form of a criminal, offense shall be given full force and effect."[189] This provision includes the utilization of MLATs and extradition treaties entered by the Philippines.[190]

In the IRR of the Cybercrime Prevention Act of 2012, the Philippines may render assistance to a foreign State on the real-time collection of data and interception thereof subject to the provision on the procurement of a valid cybercrime warrant.[191] Furthermore, the IRR only allows a foreign State to conduct two things:

> (1) [a]ccess publicly available stored computer data located in the country or elsewhere; or
>
> (2) [a]ccess or receive, through a computer system located in the country, stored computer data located in another country, if the other State obtains the lawful and voluntary consent of the person who has the lawful authority to disclose the data to said other State through that computer system.[192]

Nowhere in the said provision or in the IRR was it said that a foreign State may conduct a search of a computer system or data in the Philippines or the consequences should a foreign State conduct the same in the Philippines.[193]

Meanwhile, the international cooperation provision of the Rule on Cybercrime Warrants pertains only to the service of warrants to persons or service providers abroad.[194] The provision says, "[f]or persons or service providers situated outside of the Philippines, service of warrants and/or other court processes shall be coursed through the Department of Justice [—] Office

189. Cybercrime Prevention Act of 2012, § 22.

190. Rules and Regulations Implementing the Cybercrime Prevention Act of 2012, Republic Act No. 10175, rule 5, § 25, para. 2 (2015).

191. *Id.* rule 5, § 25, para. 2, (a)–(b).

192. *Id.* rule 5, § 25, para. 2, (c) (1)-(2).

193. *See generally* Rules and Regulations Implementing the Cybercrime Prevention Act of 2012, rule 5, § 25.

194. RULE ON CYBERCRIME WARRANTS, § 2.8.

of Cybercrime, in line with all relevant international instruments and/or agreements on the matter."[195]

Does the provision mean that a WDCD, WICD, WSSECD, or WECD must first be issued before electronic evidence can be transmitted to the Philippines and thereafter be admitted as evidence in a court of law? In other words, is a cybercrime warrant a precondition to request assistance from a foreign State under the provisions of an existing MLAT? Or does the provision contemplate a mere notice to the person or service provider that computer data in the Philippines that he, she, or it preserves will be subject to disclosure, interception, search, seizure, or examination?

2. The *Gorshkov* Case

The notorious case of *U.S. v. Gorshkov* involves a hacking scheme conducted by two Russian Nationals, Alexey Ivanov and Vasiliy Vyacheslavovich Gorshkov.[196] The Federal Bureau of Investigation (FBI) set up Ivanov and Gorshkov to go to Seattle and access their personal computer in Russia via an FBI-owned computer in Seattle to demonstrate their hacking skills.[197] The FBI then used a program to record the Russians' passwords and usernames while they were logging in via the FBI's computer.[198] After they demonstrated their hacking prowess, they were arrested.[199] Thereafter, the FBI remotely accessed Gorshkov's computer from the U.S. by using the recorded information.[200] The FBI, in accessing Gorshkov's computer, downloaded the contents thereof, but it did not read the files until a search warrant was obtained.[201]

Gorshkov questions the validity of the search and seizure of his computer files in Russia, saying that it violated his privacy rights under the U.S. Constitution.[202] The District Court ruled in the negative and said that he does not have an expectation of privacy because he entered his username and

195. *Id.* (citing Cybercrime Prevention Act of 2012, §§ 22-23).

196. Gorshkov, 2001 WL 1024026 at *1.

197. *Id.*

198. *Id.*

199. *Id.*

200. *Id.* In other words, the Federal Bureau of Investigation (FBI) hacked a computer in Russia using a computer in the U.S.

201. *Id.*

202. *Gorshkov*, 2001 WL 1024026 at *1-2.

password in the presence of FBI agents and the agents were looking over his shoulders.[203]

Furthermore, Gorshkov cannot invoke the provision of the U.S. Constitution against unreasonable search and seizure because the search was not made within the U.S. territory and he is neither a resident nor a citizen of the U.S., thus, the constitutional provision does not apply to him.[204] Additionally, the Court said that there was no seizure as the data remained intact and his possessory right over the data remained unaltered because the FBI merely copied the data.[205]

The *Gorshkov* case garnered criticism because of the peculiar — if not improper — exercise of law enforcement powers by the U.S. — which the U.S. Court justified by citing a prior case.[206]

After the "hacking" of the FBI of the Russian computer, the Russian government indicted Michael Schuler, the FBI agent who hacked the Russian computer, for unauthorized access of computer information.[207] Susan W. Brenner, a scholar on ICT law, said that the *Gorshkov* case and the actions of the FBI thereto turned the relationship of the FBI with Russian LEAs sour.[208] Furthermore, it is her shared position that the acts of the U.S. through the FBI violated Russia's sovereignty.[209]

3. Microsoft Warrant Case Series

Another case that tackled the issue on remote or transnational searches and seizures is the *Microsoft Warrant* case series.[210] A U.S. Court issued a warrant

203. *Id.* at *2.

204. *Id.* at *2-3 (citing U.S. v. Verdugo-Urquidez, 494 U.S. 259 (1990)).

205. *Gorshkov*, 2001 WL 1024026 at *3.

206. *Id.* at *2-3 (citing *Verdugo-Urquidez*, 494 U.S.).

207. Mike Brunker, *FBI agent charged with hacking: Russia alleges agent broke law by downloading evidence*, NBC NEWS, Aug. 15, 2002, *available at* http://www.nbcnews.com/id/3078784#.XSrc45MzbOQ (last accessed Nov. 30, 2020).

208. SUSAN W. BRENNER, CYBERTHREATS AND THE DECLINE OF THE NATION-STATE 48 (2009).

209. *Id.* at 53-54 (citing Nicolai Seitz, *Transborder Search: A New Perspective in Law Enforcement?*, 7 YALE J.L. & TECH. 23, 49 (2005)).

210. In re Warrant to Search a Certain E-mail Account Controlled & Maintained by Microsoft Corp., 15 F. Supp. 3d 466 (S.D.N.Y. 2014) (U.S.); Microsoft Corp v.

to search a certain e-mail account against Microsoft Corporation, which basically required Microsoft to disclose the data that it has over a certain user.[211] Microsoft refused to comply because (1) the data sought to be disclosed are located in Microsoft's facility in Ireland and (2) the warrant has no extraterritorial effect.[212] Microsoft moved to quash the warrant on the same bases, but the District Court denied the motion to quash because the Stored Communications Act (SCA) allows the extraterritorial effect of the warrants.[213]

On appeal, the same issues were tackled, but this time the Government of Ireland commented on the appeal, saying that an MLAT is the proper method in conducting the questioned law enforcement activities.[214] The Second Circuit of the U.S. Court of Appeals reversed the decision of the District Court and quashed the warrant because the language of the SCA does not grant the extraterritorial application of the warrant and the presumption against extraterritoriality stands.[215] Hence, the U.S. Court is not in a position to order Microsoft to disclose the data stored in Ireland via a warrant under the SCA.[216]

In rejecting the logic of the District Court that the Section 442 (1) (a) of the Restatement of Foreign Relations Law applies in cases where the U.S. has no MLAT with a State, the U.S. Court of Appeals said that an MLA is still a proper venue to request the disclosure of the data stored abroad for comity purposes.[217] Additionally, the U.S. Court of Appeals said —

---

U.S., 829 F. 3d 197 (2d Cir. 2016) (U.S.); & U.S. v. Microsoft Corp., 138 S. Ct. 1186 (2018) (U.S.).

211. *In re Warrant to Search a Certain E-mail Account*, 15 F. Supp. 3d at 467.

212. *Id.* at 467-68 & 470.

213. *Id.* at 477.

214. Jennifer Daskal, *The Un-Territoriality of Data*, 125 YALE L.J. 326, 393 (2015) (citing Brief of Ireland as *Amicus Curiae* Supporting Appellants at 4-7, *Microsoft Corp.*, 829 F. 3d).

215. *Microsoft Corp.*, 829 F.3d at 220-21.

216. *Id.* at 222.

217. *Id.* at 221. The Restatement of Foreign Relations Law says —

> A court or agency in the [U.S.], when authorized by statute or rule of court, may order a person subject to its jurisdiction to produce documents, objects, or other information relevant to an action or investigation, even if the information or the person in possession of the information is outside the [U.S.].

> [The U.S. Court of Appeals] find[s] it difficult to dismiss those interests out of hand on the theory that the foreign sovereign's interests are unaffected when a [U.S.] judge issues an order requiring a service provider to 'collect' from servers located overseas and 'import' into the [U.S.] data, *possibly belonging to a foreign citizen, simply because the service provider has a base of operations within the* [*U.S.*].[218]

In other words, a Court cannot compel disclosure of stored data abroad merely because it can exercise jurisdiction over the Internet Service Provider (ISP) within its territory.[219] The U.S. government filed a petition for certiorari on the Court of Appeals decision, but the Supreme Court declared the issue moot because a new warrant was already issued on the basis of the Clarifying Lawful Overseas Use of Data Act (CLOUD Act), which gives jurisdiction to a court to order an ISP or person to disclose data regardless of the data's location.[220]

4. U.K. and German Experiences

In Germany, its Federal Constitutional Court declared unconstitutional a law that allows remote searches and seizures even if a German LEA is equipped with a search warrant duly issued by a German Court on the basis that there is a right to "confidentiality and integrity" of information.[221] Meanwhile, in the U.K., a transnational LEA is allowed to conduct a remote search and seizure if it is shown that "(i) it is 'in the interests of national security'; (ii) to prevent or detect 'serious crime'; or (iii) it is 'in the interests of the economic well-being of the United Kingdom.' Intrusive surveillance can be authorized even if it 'includes conduct outside the United Kingdom.'"[222]

Susan W. Brenner is of the position that the determination whether a court will admit the evidence obtained through transnational search and seizure depends on the fact whether the LEA of the country of that court is

---

RESTATEMENT (3D) OF FOREIGN RELATIONS LAW, *supra* note 68, § 442 (1) (a).

218. *Microsoft Corp.*, 829 F. 3d at 221 (emphasis supplied).

219. *Id.*

220. *Microsoft Corp.*, 138 S. Ct. at 1187-88 (citing the Stored Communications Act, 18 U.S.C. § 2701 (U.S.) (as amended)).

221. Susan W. Brenner, *Law, Dissonance, and Remote Computer Searches*, 14 N.C. J.L. & Tech. 43, 84 (2012) (citing Wiebke Abel & Burkhard Schafer, *The German "Federal Trojan" — Challenges between Law and Technology*, 2 TEUTAS L. & TECH. 30-44 (2009)).

222. Brenner, *supra* note 221, at 85 (citing the Regulation of Investigatory Powers Act [RIPA], §§ 26 (3), 27 (3), 32 (1), 32 (2), & 32 (3) (2000) (U.K.)).

allowed by its laws to conduct transnational searches and seizures.[223] Thus, if the Philippine LEAs are not allowed to conduct remote searches and seizures, then the evidence obtained by U.S. LEA through remote search and seizure in the Philippines is not admissible in evidence in a Philippine court.[224]

Furthermore, the conduct of transnational or remote searches and seizures without the consent of the State where the search and seizure occurred violates the obligation of the searching State under MLATs.[225]

5. Section Summary

With the above, the following can be concluded:

(1) A State, in conducting transnational law enforcement, must follow the MLATs or MLA request procedure it has established with another State;[226]

(2) A State who conducted a remote search and seizure without the consent of the State where the searched computer was situated violates the territorial integrity of another State;[227]

(3) A State can conduct LE activities outside its territory if there is an extraterritorial application of its laws and its constitution allows it to do so;[228] and

(4) The determination whether evidence obtained via transnational LE that was done without the consent of the other State is

223. Brenner, *supra* note 221, at 87-88.

224. *See id*.

225. *See* Seitz, *supra* note 209, at 39-40 (wherein it was said that "[t]he procedure [in conducting remote searches and seizure without the consent of the other State] violates existing agreements on legal assistance").

226. Cybercrime Prevention Act of 2012, § 22 & Seitz, *supra* note 209, at 39-40.

227. *See* U.N. CHARTER, art. 2 (4).

228. Brenner, *supra* note 221, at 85 (citing Regulation of Investigatory Powers Act [RIPA], §§ 26 (3), 27 (3), 32 (1), 32 (2), & 32 (3) (2000) (U.K.)). *See* An Act Protecting Individual Personal Information in Information and Communications Systems in the Government and the Private Sector, Creating for This Purpose a National Privacy Commission, and for Other Purposes [Data Privacy Act of 2012], Republic Act No. 10173, § 6 (2012) (where the Philippines allowed the extraterritorial enforcement of data privacy right violations).

admissible depends on the laws of the State where the evidence is presented.[229]

## IV. QUESTIONING TRANSNATIONAL CYBER SEARCHES AND SEIZURES

With all the concepts discussed above, this Chapter synthesizes those concepts in light of the problem presented in this Note. This Chapter presents the synthesis in a "step-by-step" manner. It must be remembered that the questions surrounding the validity of transnational cyber searches and seizures are fact-heavy. Furthermore, the presumption that the evidence obtained through the search and seizure will be used in a criminal prosecution in the Philippines.

Below are the guide questions in the analyses:

(1) Can a person whose computer system was searched by a foreign State question the validity of the search and seizure or move for the exclusion of the evidence?

(2) Does the *situs* of the offense or location of the data at the time of the search and seizure matter in determining the governing law?

(3) If the *situs* is material, which law governs in determining the validity of the search and seizure?

### *A. First Step: Determination of Standing*

The question as to whether a person has standing has been resolved by Philippine jurisprudence. As mentioned above, the person questioning the admissibility of evidence on the basis of the legality of the search and seizure must be the one whose right to privacy was violated.[230]

In the context of transnational cybercrime, the person who has standing to question the search and seizure conducted against him or her depends on the method of the search and seizure used. Thus:

(1) If the search and seizure were conducted via disclosure of computer data by an ISP, the ISP and the service subscriber may question the search and seizure;[231]

229. *Compare* Brenner, *supra* note 221, at 84 (citing Abel & Schafer, *supra* note 221, at 30-44) *with* Brenner, *supra* note 221, at 85 (RIPA, §§ 26 (3), 27 (3), 32 (1), 32 (2), & 32 (3)).

230. *Stonehill*, 20 SCRA at 390 (citing Lesis vs. U.S., 6 F. 2d. 22 (1925) (U.S.)).

231. *See* RULE ON CYBERCRIME WARRANT, § 4.2 (wherein the basic information of a person or an Internet Service Provider (ISP) is required to be mentioned in the

(2) If the search and seizure were conducted via interception of computer data, the person who is a party to the communication or correspondence may question the validity of the search and seizure;[232] and

(3) If the search and seizure were conducted via search, seizure, and examination of computer data, the owner of the device that will be examined for its contents may question the validity of the search and seizure.[233]

The issue whether the admissibility of evidence obtained via an MLAT may be questioned has been discussed above, i.e., (1) because of the unequal treatment of the MLATs to persons, a person who was searched via an MLAT may nevertheless question the search and seizure made to him or her even if the MLAT expressly says that he or she has no right to do so and (2) because the Supreme Court had invoked its rule-making power in regard to how MLATs operate, the Supreme Court may again invoke this power to provide a legal standing, which is procedural in nature, for persons who were searched via an MLAT.

### *B. Second Step: Determination of Situs of the Search and Seizure*

The determination of the *situs* of the search and seizure is crucial in determining the subsequent questions. The *situs* of the search and seizure depends on technical aspects (e.g., the location of the data source, where can it be accessed, where it was targeted, where it has effects, and the technique used by the LEA).

#### 1. Remote Searching the Data Source

It is easy to determine the *situs* if the method used is the remote search and seizure conducted on the data source. This is exactly what happened in the case of *Gorshkov*, where the FBI searched a computer in Russia via a computer in U.S.[234] In the said case, the U.S. Court considered that the search and seizure occurred in Russia because the data searched and seized was in Russia.[235] This is somewhat affirmed in the *Microsoft* cases where the U.S.

application for warrant) & *Disini, Jr.*, 716 SCRA at 459 (J. Carpio, concurring and dissenting opinion).

232. *Id.*

233. *Id.*

234. *Gorshkov*, 2001 WL 1024026 at *1.

235. *Id.* at *2–3 (citing *Verdugo-Urquldez,* 494 U.S. at 259).

Court said that the CLOUD Act allowed the search and seizure of a computer system located abroad, which is in exercise of extraterritorial jurisdiction.[236] That is also what occurred in Germany and in the U.K.[237]

In the case of the Philippines, if a computer system is located in the Philippines and the data searched and seized is one that is stored in that computer system, the *situs* of the search and seizure is the Philippines.[238]

2. Interception of Data Transmitted

Interception "refers to listening to, recording, monitoring or surveillance of the content of communications, including procuring of the content data, either directly, through access and use of a computer system, or indirectly through the use of electronic eavesdropping or tapping devices, at the same time that the communication is occurring."[239] Thus, the invocation of the accessibility approach, targeting approach, or effects doctrine to the law enforcement against cybercrimes may require the use of interception because these approaches have the perspective that a cybercrime is occurring in the State that wants to exercise jurisdiction.[240]

In the accessibility approach, an act is presumed to have occurred in the territory of a State if the act can be accessed from that State.[241] Thus, if the data was roaming around the cyberspace and may be accessed in the Philippines, the search and seizure of such data via interception may be considered to have been made in the Philippines because of the accessibility approach.[242]

In the targeting approach, an act has presumably occurred in another State if it is targeted at that State.[243] Hence, if the data is sent to the Philippines because the sender sends something to a person here in the Philippines, the

236. *Microsoft Corp.*, 138 S. Ct. at 1187-88 (citing the Stored Communications Act, 18 U.S.C. 2701 (U.S.) (as amended)).

237. Brenner, *supra* note 221, at 85 (citing Abel & Schafer, *supra* note 221, at 30-44 & RIPA, c. 23, §§ 26 (3), 27 (3), 32 (1), 32 (2), & 32 (3)).

238. *See id.*

239. RULE ON CYBERCRIME WARRANTS, § 1.4 (k) (citing Cybercrime Prevention Act of 2012, § 3 (m) & Rules and Regulations Implementing the Cybercrime Prevention Act of 2012, rule I, § 3 (aa) (2015)).

240. *See generally* Kohl, *supra* note 36, at 38-49.

241. *See* Kohl, *supra* note 36, at 38.

242. *Id.*

243. *Id.* at 45.

interception made by Philippine LEA of such data is considered to have occurred in the Philippines.[244] In the same vein, if the data is sent to U.S. from the Philippines and the U.S. LEA intercepted that data, the interception is made in the U.S. because the data is targeted to the U.S.[245]

On the other hand, a State's invocation of the effects doctrine in exercising jurisdiction affects the determination of the *situs* on the basis of the State's action towards that effect.[246] Thus, if the State conducts an interception as a preventive measure, the doctrines similar to the accessibility and targeting approaches may apply.[247] But if the State conducts remote search and seizure of a computer abroad as a preventive measure, the *situs* may be presumed to be in that foreign State.[248]

### *C. Third Step: Determination of State's Consent, the Actor, and the Applicable Law*

The next question that has to be answered is the determination as to who conducted the search and seizure then the determination of the consent of the States involved in the transnational searches and seizures. Once the identity of the actor and the State consent has been determined, the applicable law will be determined.

This Section is divided into two parts, namely: searches done in the Philippines and searches done outside the Philippines.

#### 1. Searches and Seizures Done in the Philippines

In the problem posted by this Note, there are two LE units involved (i.e., the Philippine LEA and foreign LEA).

##### *a. Searches and Seizures Done by Philippine LEA*

For obvious reasons, any cyber search and seizure made by a Philippine LEA within the Philippines is governed by Philippine law. Thus, the doctrines set forth in *Disini, Jr.* and the guidelines laid down in the Rule on Cybercrime

244. *Id.*

245. *Id.*

246. This is because the effects doctrine presupposes that most (if not all) the elements of the offense occurred abroad and the effects or results thereof are felt in the State. *See* Kohl, *supra* note 36, at 48 (citing *SS Lotus*, 1927 P.C.I.J., at 23).

247. *See* Kohl, *supra* note 36, at 38 & 45.

248. *See* Brenner, *supra* note 221, at 85 (citing Abel & Schafer, *supra* note 221, at 30–44 & RIPA, c. 23, §§ 26 (3), 27 (3), 32 (1), 32 (2), & 32 (3)).

Warrants apply.[249] As an example, if a Philippine LEA intercepts data coming from the U.S. to the Philippines, the Philippine LEA must comply first with the requirements under the Rule on Cybercrime Warrants, so that he, she, or it can validly record the data sent from the U.S. to the Philippines.[250]

*b. Searches and Seizures Done by Foreign LEA*

In cases where the searches and seizures were done in the Philippines and the actor is a foreign LEA, the consent of the Philippines is material. For the purposes of discussion, this point will be divided into two (i.e., when the Philippine government consented to the search and seizure and when the Philippine government did not consent to the search and seizure).

i. Consent was given

If the consent of the Philippine government was given in order for a foreign LEA to conduct a search and seizure of a computer system in the Philippines or to intercept data that will be transmitted to the Philippines, where the purpose of the search and seizure, among others, is to obtain evidence to be used in a subsequent prosecution of a criminal case in the Philippines, the foreign LEA has to be characterized as a state agent of the Philippines.[251] The reason for that is the foreign LEA performs an act that is "under the color of a state-related function."[252] To clarify, it is the consent of the Philippines that determines the character of the foreign LEA as agents of the Philippines and not mainly on the fact that the *situs* of the search is the Philippines.

As an example, a foreign LEA visited the Philippines to investigate a cybercrime here in the Philippines, and the foreign LEA actively coordinated with the local LEA to investigate a criminal in the Philippines.[253] The foreign LEA is considered as a state-agent of the Philippines because he or she is acting

249. *See generally Disini, Jr.*, 716 SCRA & RULE ON CYBERCRIME WARRANTS.

250. *Id.*

251. *See generally Miguel*, 833 SCRA.

252. *Id.* at 449 (citing *Dela Cruz*, 779 SCRA at 60-61 (2016)).

253. *See, e.g.*, 60 Minutes Australia, Video, *60 Minutes Australia | Catching a Monster, Part one (2015)*, Jan. 22, 2018, YOUTUBE, *available at* https://www.youtube.com/watch?v=YI33EPlCW5w (last accessed Nov. 30, 2020) (interview with foreign LEA begins at 2:50).

"under the color of a state-related function [of the Philippines]."[254] Any and all acts done by that foreign LEA may be attributed to the Philippines.

In another situation, if the Philippines, by virtue of an MLAT, requests a foreign LEA abroad to conduct a search and seizure of a computer system, which stores the data obtained here in the Philippines (probably on the reason that the Philippines lacks the technology to conduct its own search and seizure of a computer data), the following can be derived:

(1) The search and seizure occurred in the Philippines;

(2) It was done with the consent of the Philippine government; and

(3) The foreign LEA, even if abroad, is presumed to be the State agent of the Philippines because the foreign LEA acts under the color of the function of the Philippine government.

ii. Consent was not given

If the consent of the Philippine government was not given and the foreign LEA conducted any remote search and seizure of a computer system in the Philippines, the foreign LEA is deemed to have violated the territorial integrity of the Philippines under international law.[255] The Philippine government may file an action against the foreign LEA because the foreign LEA has committed an unlawful access of data in the Philippines in the same way as the Russian government went after the FBI agent who conducted the search and seizure in the *Gorshkov* case.[256]

The reasons why the Philippines may prosecute a claim against the foreign LEA are:

(1) The Philippines punishes the unauthorized interference of the computer data;[257] and

(2) The act of the foreign LEA is targeted at the Philippines, which means that the act is made in the Philippines.[258]

254. *Miguel*, 833 SCRA at 449.

255. *See* U.N. CHARTER, art. 2, ¶ 4.

256. *See* Brunker, *supra* note 207.

257. Cybercrime Prevention Act of 2012, ch. II, § 4 (a) (1) & (2).

258. *See* Kohl, *supra* note 36, at 45.

2. Searches and Seizures Done Outside the Philippines

For searches and seizures done outside the Philippines, again, there are two actors (i.e., Philippine LEA and foreign LEA).

*a. Searches and Seizures by Philippine LEA Abroad*

Practically speaking, the Philippines is actually the State that is being assisted by a foreign LEA in the investigation and LE against cybercrimes.[259] However, this Note does not foreclose the possibility that the Philippines may someday conduct LE activities in another State in that regard. Hence, this discussion is a theoretical approach should the Philippine LEA conduct LE activities outside the country to prosecute a case here in the Philippines.

If the Philippine LEA asked or requested if it could conduct LE activities in a foreign State via an MLAT (which generally says that in a search and seizure, the law of the Requested State will govern) and the latter consented thereto, the Philippine LEA is considered to be acting as an agent for that foreign State because by definition, a State agent is one who "act[ed] under the color of a state-related function."[260] As mentioned, a foreign LEA who conducts LE activities in the Philippines with the State's consent is an agent of the Philippine government.[261] In the same vein, a Philippine LEA allowed to conduct any search and seizure in a foreign State should be considered as an agent of that foreign State because that Philippine LEA acted under the color of a state-related function of that State; thus, the acts of that LEA are bound by the act of state doctrine.[262]

The Cybercrime Prevention Act of 2012 provides that the treaties and other international law instruments must be utilized to the widest extent possible in combatting cybercrimes. [263] This provision recognizes the obligation of the Philippines to undergo the MLA processes in assisting and requesting for assistance in LE activities concerning cybercrimes.[264] Thus, it necessarily follows that when Philippine LEAs conduct searches and seizures abroad without the consent of the State where the searches and seizures are made, the acts of Philippine LEAs are in violation of the Cybercrime Prevention Act of 2012. Not only are they in violation of the law, they are

259. *See, e.g.*, 60 Minutes Australia, *supra* note 253.

260. *Miguel*, 833 SCRA at 449 (citing *Dela Cruz*, 779 SCRA at 60-61).

261. *See id*.

262. *Id*. *See also Banco Nacional de Cuba*, 376 U.S. at 401.

263. Cybercrime Prevention Act of 2012, § 22.

264. *Id*.

also in violation of the international law obligations of the Philippines.[265] However, the protections extended under the Constitution and other laws to individuals have no extraterritorial reach.[266] In this case, the prosecutor can successfully invoke the principle of *male captus*, *bene detentus* wherein LE activities of Philippine LEAs abroad may not be questioned if there is no law providing for the standing to question said activities.[267]

*b. Searches and Seizures Done by Foreign LEA Within Their Territory*

Finally, what would be analyzed now are searches and seizures done by foreign LEAs within their territory. For purposes of discussion, this portion will be divided into two: (1) when the search and seizure were done by an MLAT request of the Philippines and (2) when the search and seizure were done by the foreign State *motu proprio*.

i. Search and Seizure Request via an MLAT

As mentioned, an MLAT may cover search and seizure activities. The provisions of the MLATs generally contain the requirement that searches and seizures must be made in accordance with the law of the Requested State.[268] While MLATs require that the request must contain the legal bases to render a request via an MLAT,[269] the rules have been modified by the Rule on Cybercrime Warrants when it requires that when "persons or service providers situated outside of the Philippines, service of warrants and/or other court processes shall be coursed through the Department of Justice [—] Office of

265. *See Bennett*, 1 A.C. at 67 & *Ebrahim*, 21 I.L.M. 888.

266. Dodge, *supra* note 170, at 88 & *Kiobel*, 569 U.S.

267. *See, e.g.*, *Ker*, 119 U.S. & *Frisbie*, 342 U.S.

268. *See* AUS-PH MLAT, *supra* note 171, art. 17 (1); U.S.-PH MLAT, *supra* note 172, art. 14 (1); China-PH MLAT, *supra* note 173, art. 13 (1); HK-PH MLAT, *supra* note 174, art. XVII (1); Swiss-PH MLAT, *supra* note 175, art. 4, (1)-(2); PH-Korea MLAT, *supra* note 177, art. 16 (1); PH-Spain MLAT, *supra* note 178, art. 16 (1); UK-PH MLAT, *supra* note 179, art. 16 (1); ASEAN MLAT, *supra* note 180, art. 18 (1); & Budapest Convention, *supra* note 22, art. 27 (3).

269. *See* AUS-PH MLAT, *supra* note 171; U.S.-PH MLAT, *supra* note 172; China-PH MLAT, *supra* note 173; HK-PH MLAT, *supra* note 174; Swiss-PH MLAT, *supra* note 175; PH-Korea MLAT, *supra* note 177; PH-Spain MLAT, *supra* note 178; UK-PH MLAT, *supra* note 179; ASEAN MLAT, *supra* note 180; & Budapest Convention, *supra* note 22.

Cybercrime, in line with all relevant international instruments and/or agreements on the matter."[270]

Does it mean therefore that when there is no cybercrime warrant that was issued prior to the sending of the MLA request, the request is deemed defective and any and all subsequent acts done thereto would be invalid? This will be answered in the next Section.

ii. Search and Seizure Done by Foreign LEA in its own Initiative

If a foreign LEA conducted search and seizure within its territory on its own initiative, the foreign LEA is subject to its State's laws because it is acting purely in the sovereign capacity of the State on whose behalf it is acting.[271]

*D. Fourth Step: Determination of Admissibility*

Since the governing law has been determined, the next thing that will be determined is whether the evidence obtained may be admissible. This Section will be divided in the same manner the previous Section was divided. According to the Rules of Evidence, "[e]vidence is admissible when it is relevant to the issue and not excluded by the Constitution, the law or [the Rules of Court]."[272]

1. Searches and Seizures in the Philippines

If the search and seizure were done in the Philippines by a Philippine LEA, the admissibility of evidence will be determined in accordance with Philippine substantive and procedural law.[273] In the same way, a foreign LEA who is acting as an agent of the Philippines by virtue of the doctrine in *Miguel*, which cited the doctrines in *Malngan*, *Lauga*, and *Dela Cruz*.[274]

On the other hand, if the foreign LEA has acted without the consent of the Philippines and the evidence was transmitted to the Philippines, the court may admit the evidence on the basis that the Constitutional principles on searches and seizures do not apply to persons who are not agents of the

270. RULE ON CYBERCRIME WARRANTS, § 2.8 (citing Cybercrime Prevention Act of 2012, §§ 22-23).

271. *See Banco Nacional de Cuba*, 376 U.S. at 401.

272. 2019 REVISED RULES ON EVIDENCE, rule 128, § 3.

273. *See generally Disini, Jr.*, 716 SCRA & RULE ON CYBERCRIME WARRANTS.

274. *Miguel*, 833 SCRA at 449-51 (citing *Malngan*, 503 SCRA at 324; *Lauga*, 615 SCRA at 549; & *Dela Cruz*, 779 SCRA at 60-61).

Philippine government.[275] The evidence is still admissible because there is no law providing for the inadmissibility of the illegally obtained evidence of a foreign State.[276]

Although one might assert that the evidence may still be inadmissible by a contemporary construction of the Anti-Wiretapping Law,[277] the rule manifested thereat is specific to recordings or interceptions done via "dictaphone or dictagraph or detectaphone or walkie-talkie or tape recorder, or however otherwise described[.]"[278] The phrase "however otherwise described" is similar to the term *et cetera* where the doctrine of *ejusdem generis* applies, i.e., "where a description of things of a particular class or kind is 'accompanied by words of a generic character, the generic words will usually be limited to things of a kindred nature with those particularly enumerated[.]'"[279]

Hence, in these instances, the only remedy for a person in the Philippines who was searched by a foreign LEA without the consent of the Philippine government is to file a claim against the officer applicable similar to the epilogue to the *Gorshkov* case.[280]

2. Searches and Seizures Done Outside the Philippines

If the search and seizure were done outside the Philippines by the Philippine LEA via an MLAT and the foreign State consented, the Philippine LEA is treated as an agent of that foreign State; in effect, the acts of Philippine LEA abroad are acts of that sovereign State, and Philippine courts cannot sit in judgment to determine the validity of the search and seizure in that State.[281]

If the search and seizure was done without the consent of the foreign State, Philippine courts may admit the evidence on the reason that the constitutional and statutory protections under Philippine law do not have

275. *Marti*, 193 SCRA at 67-68.

276. *See* REVISED RULES ON EVIDENCE, rule 128, § 3.

277. *See* An Act to Prohibit and Penalize Wire Tapping and Other Related Violations of the Privacy of Communication, and for Other Purposes, Republic Act No. 4200, § 4 (1965) (also known as the Anti-Wiretapping Law).

278. Republic Act No. 4200, § 1 (also known as the Anti-Wiretapping Law).

279. Philippine Bank of Communications v. Court of Appeals, 253 SCRA 241, 254 (1996).

280. *See* Brunker, *supra* note 207.

281. *See Miguel*, 833 SCRA at 449 (citing *Dela Cruz*, 779 SCRA at 60-61); & *Banco Nacional de Cuba*, 376 U.S. at 401.

extraterritorial application.[282] Furthermore, any invocation that the law of the foreign State explicitly says that the evidence illegally obtained by individuals, regardless of whether they are acting on behalf of that State, is inadmissible must be disregarded by Philippine courts, even upon proof of that law, because the rule on admissibility of evidence is procedural in nature and does not call for the application of a foreign law.[283]

On the other hand, if a foreign LEA conducted a search and seizure within its territory by virtue of an MLA request, the act of state doctrine applies,[284] i.e., the Philippine Court will not sit to judge the validity of the acts of the foreign LEA done within its territory.[285] If there is no cybercrime warrant that was issued prior to the MLA request, the request shall remain valid and evidence obtained from the execution of the request enjoys the presumption of validity under the act of state doctrine.[286]

The act of state doctrine also applies to a situation when a foreign LEA has done a search and seizure in its own initiative within its territory.[287]

## V. SUMMARY AND CONCLUSION

Regardless of the nature of the no-standing provision, i.e., whether it is absolute, the law governing the search and seizure differs depending on the *situs* of the search and seizure, the actor thereof, and the consent of the State where the search and seizure occurred, i.e.,:

(1) If the *situs* is the Philippines and the actor is an agent of the Philippine government, the law governing the search is Philippine law;

(2) If the *situs* is the Philippines and the actor is a foreign State who acted without the consent of the Philippines, the evidence may be admitted because the actor is not a State agent, without

282. *See Gorshkov*, 2001 WL 1024026 at *2-3 (citing *Verdugo-Urquidez*, 494 U.S. at 260).

283. *See* JOVITO R. SALONGA, PRIVATE INTERNATIONAL LAW 130-31 (1995) (citing RESTATEMENT (1ST) OF CONFLICT OF LAWS, § 584 (1934) & RESTATEMENT (2D) OF CONFLICT OF LAWS, §§ 122-143 (1965)).

284. *Banco Nacional de Cuba*, 376 U.S. at 401.

285. *See Banco Nacional de Cuba*, 376 U.S. at 416 (citing Underhill v. Hernandez 168 U.S. 250, 252 (1897)).

286. *Id.* at 401.

287. *Id.*

prejudice to the liability of the officer who committed the act of unlawful search and seizure;

(3) If the *situs* is the foreign State and the actor is an agent of the Philippines and it was done with the consent of the foreign State, the act of state doctrine applies;

(4) If the *situs* is the foreign State and the actor is an agent of the Philippines and it was done without the consent of the foreign State, the evidence will be treated the same way as a foreign LEA who has done search and seizure in the Philippines without the consent of the Philippines, and constitutional and statutory protections under Philippine laws do not have extraterritorial reach; and

(5) If the *situs* is the foreign State and the actor is an agent of that foreign State, the law governing the search is that foreign State's law. In this case, the act of state doctrine may apply.

*A. No-Standing and Its Implication*

Even if one would uphold the view that the language does prohibit the questioning of a search conducted via an MLAT absolutely, the validity of the no-Standing provision cannot be sustained because these provisions found on different treaties violate the equal protection clause. As mentioned, almost half of the MLATs entered by the Philippines do not contain a no-standing provision, and there is no difference between a person who was searched by a foreign LEA whose MLAT with the Philippines contains the supposed no-standing provision and another person who was searched by another foreign LEA whose MLAT with the Philippines does not contain the supposed no-standing provision. In this case, the accused, subject to the requirements of standing vis-à-vis his or her privacy rights, may question the search. The basis to question would be the rules of evidence, conflict of laws doctrines, and the Budapest Convention. Furthermore, the ruling in *People v. Sergio*[288] implies that the MLATs' provisions, especially when they involve evidence, are subject to the provisions of the Rules of Court.[289]

288. People v. Sergio, G.R. No. 240053, Oct. 9, 2019, *available at* http://sc.judiciary.gov.ph/7732 (last accessed Nov. 30, 2020).

289. *Id.* at 17-19.

*B. Law Governing the Search and Seizure*

Provided that a person has standing to question a search vis-à-vis his or her privacy rights, he or she may question the search conducted against him or her.

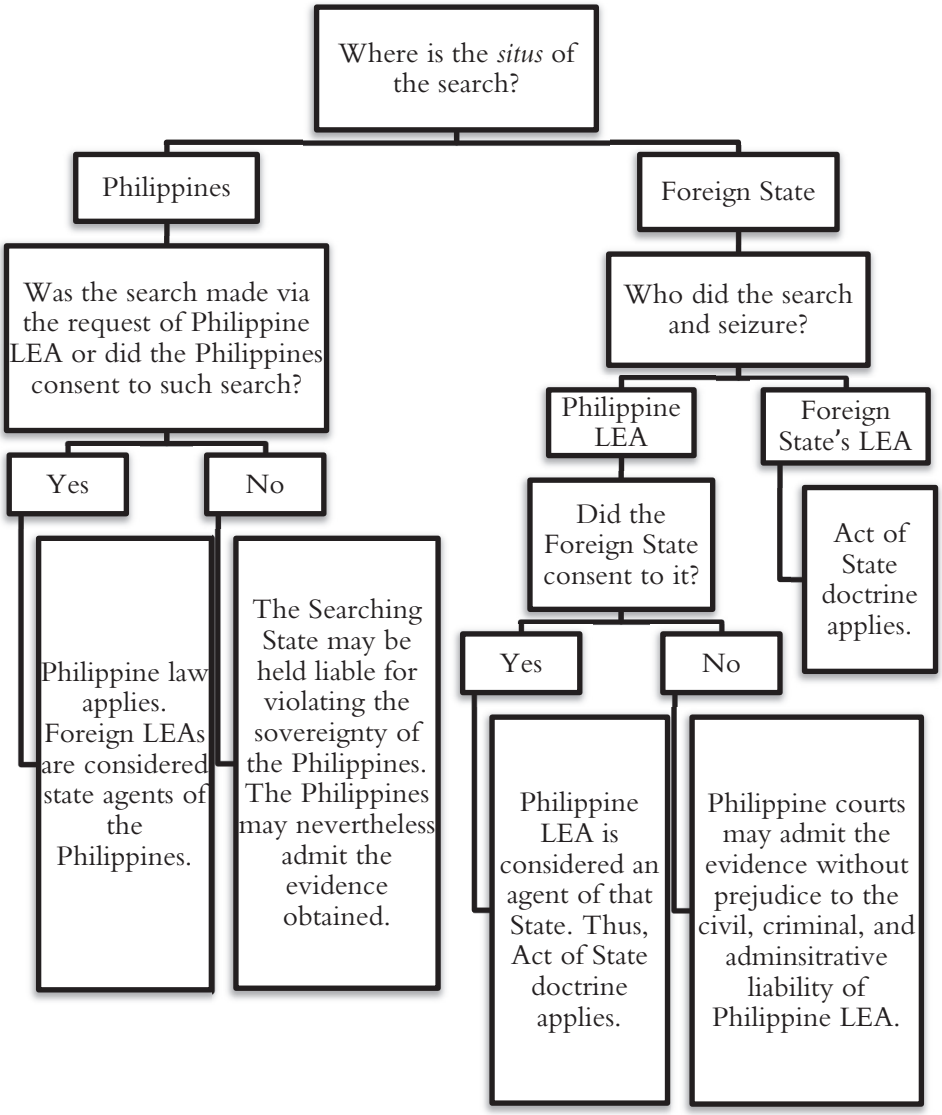
In questioning the search, a court must first determine the *situs* of the search. The determination of *situs* begins with the determination how the data was obtained. If the data was obtained via real time collection of data, the search is deemed to have been made where the law enforcers intercepted the data. If the data was obtained via the accessing of the accused's computer systems in the foreign State, the *situs* is that foreign State.

The second determination that the court must do is whether a State consented to the search. If the Philippines consented to the search made by foreign LEAs in the Philippines, the foreign LEAs are considered agents of the Philippines. If the foreign State consented to the search made by Philippine LEAs within their territory (via an MLAT), the Philippine LEAs are considered to be agents of that State; thus, the act of state doctrine applies.

If consent was not given by the Philippines when the foreign LEA conducted the search in the Philippines, Philippine courts may admit the evidence without prejudice to a claim against the foreign LEA who conducted the search. In the same vein, if the foreign State did not consent to the LE activities of Philippine LEAs in its territory, the evidence obtained by Philippine LEA may be admitted in a court in the Philippines.

Finally, if the search conducted by the foreign LEA was made within its jurisdiction, the court must assume that the act of state doctrine applies. Below is the diagram of questions and answers mentioned above[290] —

290. The Author also formulated a manual for judges in examining remote searches and seizures in the latter part of this Note.


Where is the *situs* of the search?
Philippines
Foreign State
Was the search made via the request of Philippine LEA or did the Philippines consent to such search?
Who did the search and seizure?
Yes
No
Philippine LEA
Foreign State's LEA
Philippine law applies. Foreign LEAs are considered state agents of the Philippines.
The Searching State may be held liable for violating the sovereignty of the Philippines. The Philippines may nevertheless admit the evidence obtained.
Did the Foreign State consent to it?
Act of State doctrine applies.
Yes
No
Philippine LEA is considered an agent of that State. Thus, Act of State doctrine applies.
Philippine courts may admit the evidence without prejudice to the civil, criminal, and adminsitrative liability of Philippine LEA.

## VI. RECOMMENDATIONS

To put an end to the complexities surrounding the issues of searches and seizures made in relation to transnational cybercrime, the following are the recommendations of the Author:

(1) There must be a procedural doctrine or rule governing the admission and presentation of evidence obtained through MLATs; and

(2) There must be a law or an amendment to existing law that will govern transnational cybercrimes.

### *A. Adoption of a Procedural Doctrine on Transnational Cybercrime Searches and Seizures*

An adoption of a procedural doctrine on transnational cybercrime searches and seizures is necessary to clarify the procedural aspects of questioning the searches and seizures conducted by a foreign State via MLAT. This doctrine must state in essence these requirements:

(1) The Philippines and the Foreign State had entered into a Mutual Legal Assistance Agreement;

(2) There was a request made by the Philippines for evidence relating to the commission of transnational cybercrime;

(3) The request was made to the foreign State;

(4) The foreign State is going to initiate search and seizure operations because of the request or to send the retrieved evidence to the Philippines that was obtained from a search and seizure operation made prior to the request; and

(5) There is a report made by the foreign LEA stating the process of search and seizure, which includes the statement that the search and seizure operation was made in accordance with the laws of the foreign State and the chain of custody of the retrieved evidence.[291]

291. *See generally* AUS-PH MLAT, *supra* note 171; U.S.-PH MLAT, *supra* note 172; China-PH MLAT, *supra* note 173; HK-PH MLAT, *supra* note 174; Swiss-PH MLAT, *supra* note 175; PH-Korea MLAT, *supra* note 177; PH-Spain MLAT, *supra* note 178; UK-PH MLAT, *supra* note 179; & ASEAN MLAT, *supra* note 180, art. 18 (1) (where the Requested State may be requested to provide a report on the methods used in searches and seizures).

*B. Governing Law on Transnational Cybercrimes and Transnational Law Enforcement*

The law governing transnational cybercrime may either be an amendment of the current Cybercrime Prevention Act of 2012 or an entirely different law. This Author, however, is of the position that an amendment of the Cybercrime Prevention Act would be more efficient than writing a new law. The amendment must first define what transnational cybercrimes are. Second, it must define the parameters of determining the *situs* of searches and seizures conducted by a foreign State. Finally, it must provide the law governing the said searches and seizures.

On this matter, it is proposed that the following must be included to amend Section 3 of the Cybercrime Prevention Act of 2012:

> (q) *Transnational cybercrime* refers to any of the offenses mentioned herein and/or the Budapest Convention on Cybercrime that is committed (1) in more than one State; (2) in one State but a substantial part of its preparation, planning, direction, or control takes place in another State; (3) in one State but involves an organized criminal group that engages in criminal activities in more than one State; or (4) in one State but has substantial effects in another State.[292]
>
> (r) *Remote searches and seizures by the Philippines* refer to searches and seizures conducted by the Philippines either *motu proprio* or via a request under any legal assistance agreement to a data originating from or stored outside the Philippines.
>
> (s) *Remote searches and seizures by a foreign State* refer to searches and seizures conducted by a foreign State either *motu proprio* or via a request under any legal assistance agreement to a data originating from or stored in the Philippines.

Furthermore, additional Sections under Chapter VI of the Cybercrime Prevention Act of 2012 must also be included to reflect the following:

> *Section 22-A. Remote Searches and Seizures; Presumptions.* — Should a foreign State conduct any search and seizure of data originating from the Philippines and sent to such State, it is presumed that the search and seizure occurred in such foreign State. Should the search and seizure concern a computer system in the Philippines, or data found in the Philippines and the data was not sent to such foreign State, it is presumed that the search and seizure occurred in the Philippines.

292. UNCTOC, *supra* note 2, art. 3, ¶ 2.

If the search and seizure occurred in the Philippines and the search and seizure were made with the consent or request of a Philippine Law Enforcement Agency, Philippine domestic laws apply.

The amendment may also declare the extraterritorial law enforcement of the Philippines to combat transnational cybercrimes, which must reconcile the obligations of the Philippines under MLATs and other international instruments. The Philippines may enact a law or amend a law that provides a mechanism similar to RIPA[293] and the CLOUD Act.[294] This results in a situation where the Philippines allows the extraterritorial application of laws, which the Philippines is not a stranger to.[295] This would also provide a regulatory mechanism on the acts done by Philippine LEAs abroad.

The governing law must also provide the regulation on the conduct of foreign LEAs who are doing LE activities in the Philippines, including joint LE activities. This may include the effect of the lack of consent of the Philippines in the LE activities to the admissibility of evidence obtained by foreign LEA from the LE activity. Thus, the following may be included:

> *Section 22-B. Transnational Law Enforcement by Philippine Law Enforcement Agents* — Philippine Law Enforcement Agents may conduct remote searches and seizures in another State *provided* that (1) a valid warrant under this Act and the relevant rule of court was obtained and (2) the consent of that State was obtained. The absence of both invalidates the search and seizure, but the absence of consent will not invalidate the acts done pursuant to the search warrant. However, the law enforcement agent who failed to secure the other State's consent may be held liable under Philippine law.
>
> *Section 22-C. Transnational Law Enforcement by Foreign Law Enforcement Agents* — Foreign Law Enforcement Agents may conduct searches and seizures in a computer system in the Philippines *provided* that the consent of the Philippines was obtained, and the requisite cyber warrant was procured prior to the search. The evidence obtained therefrom is likewise admissible in the Philippines. The absence of consent will not affect the admissibility of evidence but may subject the foreign law enforcement officer who conducted the search and seizure to criminal prosecution under relevant Philippine laws, but if consent was given and there is no valid warrant, the evidence is inadmissible.
>
> *Section 22-D. Joint Law Enforcement Activities* — If Foreign Law Enforcement Agents are partnered with Philippine Law Enforcement Agents to conduct

293. *See generally* RIPA, §§ 26 (3), 27 (3), 32 (1), 32 (2), & 32 (3).

294. Stored Communications Act, 18 U.S.C. § 2701 (U.S.) (as amended).

295. *See* Data Privacy Act of 2012, § 6 & Budapest Convention, *supra* note 4, ch. 2, § 3, art. 22.

investigations and other forms of evidence-gathering with regard to the commission of a cybercrime, a cybercrime warrant shall be required regardless of the location of the computer system as long as any part of the law enforcement activity involved will occur within the Philippines.[296]

*C. Examining Remote Searches and Seizures: A Guide for Judges*

| Searching Authority | Did the Philippines Consent? | Method of Search and Seizure | Where was the data searched and seized stored? | Where was the data searched and seized sent? | Rules |
|---|---|---|---|---|---|
| PNP/NBI | Yes | Hacking | Philippines | N/A | Philippine Laws and Constitution may be invoked. |
| PNP/NBI | Yes | Reception or real-time collection of data | Philippines | Abroad | Philippine Laws and Constitution may be invoked because of the origin approach. |
| PNP/NBI | Yes | Hacking | Abroad | N/A | There might be a liability under the Cybercrime Prevention Act. Evidence may be admissible as the Constitutional right against unreasonable search and seizure does not have extraterritorial application. |

296. A draft of the proposed amendatory law is provided in the latter part of this Note.

| | | | | | |
|---|---|---|---|---|---|
| PNP/NBI | Yes | Reception or real-time collection of data | Abroad | Philippines | Philippine Laws and Constitution may be invoked. |
| Foreign Law Enforcement Agents (FLEAs) | Yes | Hacking | Philippines | N/A | Philippine Laws and Constitution may be invoked. FLEAs are deemed agents of the Philippines. |
| FLEAs | Yes | Reception or real-time collection of data | Philippines | Abroad | Law of the foreign State —act of state Doctrine Applies |
| FLEAs | Yes | Reception or real-time collection of data | Abroad | Philippines | Foreign law applies because of the origin approach. |
| FLEAs | No | Hacking | Philippines | N/A | Philippine Law applies, i.e., the evidence may be admitted, but subject to liability under the Cybercrime Prevention Act |
| FLEAs | No | Reception or real-time collection of data | Abroad | Philippines | Foreign laws apply because of the origin approach. |

| | | | | | |
|---|---|---|---|---|---|
| FLEAs | No | Reception or real-time collection of data | Philippines | Abroad | Law of the foreign State —act of state Doctrine Applies |
| FLEAs | No | Hacking | Abroad | N/A | Law of the foreign State — act of state Doctrine Applies |

*D. Proposed Amendatory Law*

Republic Act No. _____

AN ACT STRENGTHENING REPUBLIC ACT NO. 10175 OR "AN ACT DEFINING CYBERCRIME, PROVIDING FOR THE PREVENTION, INVESTIGATION, SUPPRESSION AND THE IMPOSITION OF PENALTIES THEREFOR AND FOR OTHER PURPOSES", OTHERWISE KNOWN AS "CYBERCRIME PREVENTION ACT OF 2012" AND APPROPRIATING FUNDS THEREFOR

Section 1. *Title* — The Title of Republic Act No. 10175 is hereby amended to "An Act Defining Cybercrime and Transnational Cybercrime, Providing for the Prevention, Investigation, Suppression and the Imposition of Penalties Therefor and for Other Purposes".

Section 2. Section 3 of Republic Act No. 10175 should now be read as follows —

> *Section 3. Definition of Terms*
>
> . . .
>
> (q) *Transnational cybercrime* refers to any of the offenses mentioned herein and/or the Budapest Convention on Cybercrime that is committed (1) in more than one State; (2) in one State but a substantial part of its preparation, planning, direction, or control takes place in another State; (3) in one State but involves an organized criminal group that engages in criminal activities

in more than one State; or (4) in one State but has substantial effects in another State.

(r) *Remote searches and seizures by the Philippines* refer to searches and seizures conducted by the Philippines either *motu proprio* or via a request under any legal assistance agreement to a data originating from or stored outside the Philippines.

(s) *Remote searches and seizures by a foreign State* refer to searches and seizures conducted by a foreign State either *motu proprio* or via a request under any legal assistance agreement to a data originating from or stored in the Philippines.

Section 3. The following sections shall be added in Chapter VI of Republic Act No. 10175 —

*Section 22-A. Remote Searches and Seizures; Presumptions.* — Should a foreign State conduct any search and seizure of data originating from the Philippines and sent to such State, it is presumed that the search and seizure occurred in such foreign State. Should the search and seizure concern a data found in the Philippines and was not sent to such foreign State, or a computer system located in the Philippines, it is presumed that the search and seizure occurred in the Philippines.

*Section 22-B. Transnational Law Enforcement by Philippine Law Enforcement Agents* — Philippine Law Enforcement Agents may conduct remote searches and seizures to another State *provided* that (1) a valid warrant under this Act and the relevant rule of court was obtained and (2) the consent of that State was obtained. The absence of both invalidates the search and seizure, but the absence of consent will not invalidate the acts done pursuant to the search warrant. However, the law enforcement agent who failed to secure the other State's consent may be held liable under Philippine law.

*Section 22-C. Transnational Law Enforcement by Foreign Law Enforcement Agents* — Foreign Law Enforcement Agents may conduct searches and

> seizures to a computer system in the Philippines *provided* that the consent of the Philippines and a cybercrime warrant were validly obtained. The evidence obtained from the search and seizure is likewise admissible in the Philippines. The absence of the consent will not affect the admissibility of evidence but may subject the foreign law enforcement officer who conducted the search and seizure for criminal prosecution under relevant Philippine laws, but if consent was given and there is no valid warrant, the evidence is inadmissible.
>
> *Section 22-D. Joint Law Enforcement Activities* — If Foreign Law Enforcement Agents partnered with Philippine Law Enforcement Agents to conduct investigations and other forms of evidence-gathering with regard to the commission of a cybercrime, a cybercrime warrant shall be required regardless of the location of the computer system as long as any part of the law enforcement activity involved will occur within the Philippines.

Section 4. *Appropriations*. — The amount of Fifty million pesos (₱50,000,000.00) shall be appropriated annually for the implementation of this Act.

Section 5. *Separability Clause*. — If any provision of this Act is held invalid, the other provisions not affected shall remain in full force and effect.

Section 6. *Repealing Clause*. — All laws, decrees or rules inconsistent with this Act are hereby repealed or modified accordingly.

Section 7. *Effectivity*. — This Act shall take effect fifteen (15) days after the completion of its publication in the Official Gazette or in at least two (2) newspapers of general circulation.