ANTONIN SCALIA LAW SCHOOL
GEORGE MASON UNIVERSITY
INTERNATIONAL LAW JOURNAL

ARTICLES:

NOTES:

VOLUME 12 SPRING ISSUE NUMBER 2

INTERNATIONAL LAW JOURNAL

VOLUME 12 | SPRING ISSUE | NUMBER 2

CONTENTS

INTERNATIONAL LAW JOURNAL

VOLUME 12 | SPRING ISSUE | NUMBER 2

INTERNATIONAL LAW JOURNAL

VOLUME 12 | SPRING ISSUE | NUMBER 2

Cite as 12 GEO. MASON INT'L L.J. ___ (2021)

The *George Mason International Law Journal* is published two times per year. The *George Mason International Law Journal* can be contacted as follows:

George Mason International Law Journal
3301 N. Fairfax Drive, Arlington, VA 22201
http://www.gmuilj.org/

The *George Mason International Law Journal* is a traditional student-edited legal periodical at the George Mason University School of Law in Arlington, Virginia. Providing international scholars and practitioners a forum to exchange, develop, and publish innovative ideas, the *Journal* is uniquely situated to address international legal issues. The *Journal* publishes scholarly, concise, and practical material from leading scholars and practitioners to provide a source of authority and analysis for the understanding and advancement of a variety of international legal topics.

Subscriptions: Single issues are available for download online at gmuilj.org. Print versions are available by request to the Managing Editor at the mail address listed above or by email at: *georgemasonilj@gmail.com*. Single issues may be purchased for $15 per copy for domestic and $18 for foreign subscribers.

Submissions: The Editors welcome submissions of unsolicited manuscripts. The *George Mason International Law Journal* seeks to publish articles and essays making a significant, original contribution to the fields concerning international topics. Footnotes should follow the form prescribed in *The Bluebook: A Uniform System of Citation* (21st ed. 2020). Articles must be both well written and completely argued at the time of submission. Manuscripts and editorial correspondence should be addressed to Senior Articles Editor, *George Mason International Law Journal*, at the address listed above or by email at: *georgemasonilj@gmail.com*

THE PROSECUTOR V. THOMAS LUBANGA DYILO: PERSISTENT EVIDENTIARY CHALLENGES FACING THE INTERNATIONAL CRIMINAL COURT

*ALIZA SHATZMAN**

I. INTRODUCTION

On March 14, 2012, Thomas Lubanga Dyilo ("Lubanga")[1] became the first individual convicted[2] by the International Criminal Court ("ICC").[3] Specifically, Lubanga was convicted of conscripting and enlisting[4] boys and girls under the age of 15,[5] and of using children under the age of 15 to participate actively in hostilities, between September 1, 2002 and August 13, 2003, in the Democratic Republic of the Congo ("DRC").[6] Lubanga was convicted under the Rome Statute ("Statute")[7] under both Article 8(2)(e)(vii) (conscripting and enlisting child soldiers) and Article 25(3)(a) (individual responsibility as a co-perpetrator).[8] Lubanga was sentenced to fourteen years' imprisonment.[9]

---

* Aliza Shatzman is a 2013 graduate of Williams College in Williamstown, Massachusetts, and a 2019 graduate of Washington University School of Law in St. Louis, Missouri. During law school, Ms. Shatzman served as an Associate Editor for the *Washington University Journal of Law and Policy*. Ms. Shatzman would like to thank her professors and mentors at Washington University School of Law, particularly Professor Leila Sadat, for encouraging her to pursue legal scholarship and to publish this Article. She would also like to thank the editors of the *George Mason International Law Journal* for their helpful feedback and suggestions.

[1] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06, Judgment (Mar. 14, 2012) [hereinafter Trial Chamber Judgment].

[2] The Special Court for Sierra Leone ("SCSL"), which was founded in 2002 to address crimes committed during the country's civil war, prosecuted and convicted several individuals for the conscription and enlistment of child soldiers before Lubanga's 2012 conviction at the ICC. *See generally* RESIDUAL SPECIAL COURT FOR SIERRA LEONE, http://www.rscsl.org/index.html (last visited Apr. 17, 2021).

[3] "The International Criminal Court (ICC) investigates and, where warranted, tries individuals charged with the gravest crimes of concern to the international community: genocide, war crimes, crimes against humanity and the crime of aggression." *See About the ICC*, ICC, https://www.icc-cpi.int/about (last visited Apr. 17, 2021).

[4] The Trial Chamber shifts between the phrases "conscripting and enlisting" and "enlisting and conscripting." The author will use the former phrase for consistency, except for direct quotes.

[5] The ICC does not have jurisdiction over individuals between ages 15 and 18. *See* Rome Statute of the International Criminal Court art. 26, July 17, 1998, 2187 U.N.T.S. 90, https://www.icc-cpi.int/resource-library/documents/rs-eng.pdf [hereinafter Rome Statute].

[6] Trial Chamber Judgment, *supra* note 1, at ¶ 1355.

[7] *See generally* Rome Statute, *supra* note 5.

[8] Trial Chamber Judgment, *supra* note 1, ¶¶ 1358-64. Lubanga was charged in 2007 under both Art. 8(2)(b)(xxvi) (war crimes of an "international" character) and Art. 8(2)(e)(vii) (war crimes of a "non-international character"); however, he was only convicted of the latter, as it was determined that the situation was of non-international character. *Id.*

[9] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-2901, Trial Chamber Decision on Sentence, ¶¶ 107-08 (July 10, 2012) [hereinafter Lubanga Decision on Sentence].

Lubanga became President of the *Union des Patriotes Congolais* ("UPC") in September 2000 and became Commander-in-Chief of the UPC's military wing, the *Forces Patriotiques pour la Liberation de Congo* ("FPLC"), when it was created in September 2002.[10] Over the next eleven months, Lubanga and his co-perpetrators "worked together and each of them made an essential contribution to the common plan that resulted in the enlistment, conscription and use of children under the age of 15 to participate actively in hostilities."[11] Furthermore, Lubanga acted with the intent and knowledge required under Art. 25(3)(a) because he was aware of both "the factual circumstances that established the existence of the armed conflict" and "the nexus between those circumstances and his own conduct, which resulted in the enlistment, conscription and use of children under the age of 15 to participate actively in hostilities."[12]

Despite overwhelming evidence that Lubanga committed the alleged crimes, the investigation and prosecution were stymied by numerous evidentiary difficulties, and the process took more than six years to complete. Nor is the *Lubanga* situation a rare instance in which issues plagued ICC prosecutors. Rather, ICC prosecutors are often hampered by evidentiary challenges: specifically, they struggle to both obtain evidence from abroad in a timely fashion and to present admissible evidence at trial.[13] Often witnesses and intermediaries are excluded based on what appear to be minor deficiencies or inconsistencies in their testimonies—despite the overwhelming predisposition for these witnesses to testify honestly.

There are many reasons for these evidentiary barriers. ICC cases often rely primarily on eyewitness testimony—which is notoriously unreliable[14]—rather than on documentary[15] or forensic evidence.[16] This

---

[10] Trial Chamber Judgment*, supra* note 1, ¶¶ 81-86 (citing UPC Statute, UPC founding documents, and Thomas Lubanga's curriculum vitae).

[11] *Id.* ¶ 1271.

[12] *Id.* ¶ 1357. Among Lubanga's "essential contributions" to the crime of conscripting and enlisting child soldiers, Lubanga (1) gave orders to and supervised senior officers who directly recruited—both voluntarily and involuntarily—child soldiers, and he was briefed frequently by these officers; (2) visited child soldier camps and gave speeches; and (3) personally utilized bodyguards who were under the age of 15. *Id.* ¶¶ 1355-56.

[13] *See generally* NANCY A. COMBS, FACT-FINDING WITHOUT FACTS: THE UNCERTAIN EVIDENTIARY FOUNDATIONS OF INTERNATIONAL CRIMINAL CONVICTIONS (Cambridge Univ. Press 2010).

[14] *See id.* As will be explored in this Article, there are many reasons for this unreliability: for example, witness trauma affects memory and perception, and the passage of time distorts recollection. *See* Joyce W. Lacy & Craig E. L. Stark, *The Neuroscience of Memory: Implications for the Courtroom*, 14(9) NAT. REVS. NEUROSCI. 649, 649-58 (2013), https://www.ncbi.nlm.nih.gov/pmc/articles/PMC4183265/pdf/nihms-624859.pdf.

[15] *See* COMBS, *supra* note 13, at 11-14. Often, individuals involved in committing war crimes do not keep records. *See id.* at 12. The Nazis were an exception to this: they kept meticulous records. *Id.* at 11.

[16] Since trials often occur many years after the crimes were committed, and due to the nature of the conflicts, it is challenging to acquire forensic evidence. *See* Nancy Amoury Combs, *Grave Crimes and Weak Evidence: A Fact-Finding Evolution in International Criminal Law*, 58 HARV. INT'L L. J. 55, 57 (2017) ("Most modern atrocities occur in places

reliance on eyewitness testimony raises questions about the credibility and reliability of witnesses, many of whom speak different languages, represent different cultures, are several years removed from the crimes, and may have been victims themselves.[17] Furthermore, it may be difficult for ICC investigators to collect testimonial evidence from remote countries.[18] Investigators put themselves at risk when they enter dangerous territory to conduct interviews with victims[19] and witnesses.[20]

Child soldier cases are especially challenging. Children are highly vulnerable to forgetting key events because of the trauma they suffered or because a significant amount of time has elapsed between the trauma and the trial.[21] Also, prosecutors may struggle to prove that the children were under the age of 15 when the crimes occurred.[22] In *Lubanga*, the co-perpetrators in the DRC did not keep records of their soldiers and prisoners, nor did the children possess birth certificates or other identification.[23] The defense in *Lubanga* challenged the credibility and reliability of many witnesses and pieces of evidence: some of whom, and some of which, were ultimately excluded.[24] In fact, at the conclusion of the trial, Lubanga challenged "the entire body of evidence presented at trial by the Prosecution."[25]

Despite significant challenges, after five years of ICC investigatory work, multiple years of Trial Chamber proceedings, meticulous determinations about witness, victim, and evidence credibility, and multiple appeals, Lubanga served a fourteen-year term of imprisonment for conscripting and enlisting children under 15 years of age to participate actively in hostilities.[26] The *Lubanga* decision was not only gratifying for those who believe in justice for victims, but it also set a precedent for future

---

that do not feature the widespread use of documentation or technology that can be so useful in proving a person's whereabouts or other basic facts.").

[17] The Trial Chamber in *Lubanga* was forced to confront allegations that some of the ICC intermediaries working with witnesses had actually coached the witnesses to lie. *See* Trial Chamber Judgment, *supra* note 1, ¶ 38. Some of these witnesses and intermediaries were ultimately excluded from the proceedings, whereas others were nevertheless deemed credible and reliable. *See id.* ¶¶ 38, 169, 1361-63.

[18] *Id.* ¶¶ 151-67; *see also* COMBS, *supra* note 13, at 147.

[19] Notably, "the victims who have been granted permission to participate in this trial are, in the main, alleged former child soldiers, although some are the parents or relatives of former child soldiers." Trial Chamber Judgment, *supra* note 1, ¶ 17. Many were granted protective status, including anonymity. *See id.* ¶ 18.

[20] *Id.* ¶¶ 151-67; *see also* COMBS, *supra* note 13, at 147.

[21] *See* COMBS, *supra* note 13, at 15; *see, e.g.*, Mark L. Howe, *Memory Development: Implications for Adults Recalling Childhood Experiences in the Courtroom*, 14 NAT. REVS. NEUROSCI. 869 (2013).

[22] Trial Chamber Judgment, *supra* note 1, ¶¶ 169-77.

[23] *Id.*

[24] *Id.* ¶¶ 37-41.

[25] *Id.* ¶¶ 119-23.

[26] Mr. Lubanga was released in March 2020. Stanis Bujakera Tshiamala, *DRC: Former Warlord Thomas Lubanga Freed After Serving 14-Year Sentence,* AFRICA REP. (Mar. 17, 2020), https://www.theafricareport.com/24712/drc-former-warlord-thomas-lubanga-freed-after-serving-14-year-sentence/.

ICC child soldier cases and offered solutions to handle the unique evidentiary challenges that such cases present.

Since the *Lubanga* decision, the ICC has successfully prosecuted two other individuals for conscripting and enlisting child soldiers—Bosco Ntaganda[27] from the DRC and Dominic Ongwen[28] from Uganda.[29] However, *three* successful child soldier prosecutions in the nearly two *decades* since the ICC was founded is not nearly enough, and many warlords across the world continue to act with impunity. The dearth of child soldier prosecutions and convictions at the ICC is a pressing issue that must be addressed.

This Article explores some of the evidentiary challenges that ICC prosecutors encountered in *Lubanga*: specifically, the difficulty of relying on eyewitness testimony in the face of barriers to presenting credible, admissible testimonial evidence. ICC prosecutions slow when witnesses cannot convey reliable information.[30] This slowdown results from factors including, but not limited to, cultural differences, linguistic and communications barriers, and memory lapses.

This Article not only offers a thorough explanation of the *Lubanga* judgment, but it also analyzes case law from the Special Court for Sierra Leone ("SCSL") and critiques the *Lubanga* decision in light of persistent challenges facing the ICC regarding child soldier cases.[31] Furthermore, the Article provides a critique of ICC evidentiary proceedings, and it offers some much-needed solutions for effective change going forward. Ultimately, this Article argues that the ICC must learn from the evidentiary challenges that arose in *Lubanga* in order to properly prosecute future child soldier cases.

II. *THE PROSECUTOR V. THOMAS LUBANGA DYILO*: PROCEDURAL HISTORY

This section describes the important aspects of the procedural history in *Lubanga*. First, it explores the preliminary investigation and the

---

[27] Prosecutor v. Ntaganda, ICC-01/04-02/06-2359, Judgment (July 8, 2019).

[28] Prosecutor v. Ongwen, ICC-02/04-01/15-1762, Trial Judgment (Feb. 4, 2021). In fact, Ongwen was conscripted and enlisted as a child soldier himself. *See Dominic Ongwen – From Child Abductee to LRA Rebel Commander,* BBC NEWS (Feb. 4, 2021), https://www.bbc.com/news/world-africa-30709581.

[29] *See Statement of ICC Prosecutor, Fatou Bensouda, on the International Day Against the Use of Child Soldiers*, *"Children's Voices and Their Stories of Unspeakable Abuses during War and Conflict Must Not Go Unheard.*," ICC (Feb. 12, 2021), https://www.icc-cpi.int/Pages/item.aspx?name=210212-prosecutor-statement.

[30] The investigative team in *Lubanga* "was subject to significant pressure, including from within the OTP as well as the Court more generally, because it was felt necessary to make progress." Trial Chamber Judgment, *supra* note 1, ¶ 134.

[31] As of February 2020, the ICC has pursued charges against five other individuals for similar crimes. *Statement of the Prosecutor of the International Criminal Court, Mrs Fatou Bensouda, on the International Day against the Use of Child Soldiers: "Children are especially vulnerable. We Must Act to Protect Them."* ICC (Feb. 12, 2020), https://www.icc-cpi.int/Pages/item.aspx?name=200212-otp-statement-child-soldiers.

charges initiated against Lubanga. Next, it illustrates the crucial aspects of the Trial Chamber's evaluation of the evidence and the elements of Article 8 crimes. Finally, this section describes Lubanga's conviction and sentencing, the appeals, and the separate opinions issued in the case.

A. Initiation, Investigation, and Evidence Collection

The UPC was created on September 15, 2000, with Lubanga as both a founding member and its first President.[32] The UPC's military wing, the FPLC, of which Lubanga was Commander-in-Chief, was founded in September 2002, at which time the FPLC seized power in Ituri.[33] Between September 2002 and August 2003, the FPLC was engaged in an internal armed conflict with multiple groups, including the *Armee Populaire Congalaise* and the *Force de Resistance Patriotique en Ituri*.[34] During this time, the FPLC's senior leadership recruited children under the age of 15 on both a voluntary and an involuntary basis.[35] The FPLC led "mobile[z]ation and recruitment campaigns" intended to persuade local families to send their children to join the fight, and it conducted "large-scale recruitment exercise[s] directed at young people…."[36]

On March 3, 2004, the Government of the DRC referred the Ituri situation to the ICC Office of the Prosecutor ("OTP").[37] On June 21, 2004, the OTP announced that it would commence an investigation into alleged war crimes committed in Ituri beginning in July 2002.[38] The investigative team working under the OTP immediately faced challenges in gathering accurate evidence in a timely fashion, yet they felt pressure to make progress quickly.[39] While the investigators worked with United Nations representatives in the field, the investigators did not always feel supported.[40] Humanitarian groups in the DRC provided reports and documentation from the region; however, because some humanitarian groups appeared to have a common agenda—to encourage the prosecution of Lubanga and other

---

[32] Trial Chamber Judgment, *supra* note 1, ¶ 81, 46/593 nn.195-96 (citing the UPC Statute, as well as UPC founding documents, and "Thomas Lubanga's *curriculum vitae* [which] indicates that he was the UPC President since 2000.").

[33] *Id.* ¶¶ 25-28.

[34] *See id.* ¶¶ 81-91, 1126-28.

[35] *See id.* ¶¶ 759-818, 1266-70.

[36] *Id.* ¶ 1354.

[37] ICC, *Case Information Sheet: Situation in the Democratic Republic of the Congo*, *The Prosecutor v. Thomas Lubanga Dyilo,* ICC-PIDS-CIS-DRC-01-017/21, https://www.icccpi.int/CaseInformationSheets/ LubangaEng.pdf (last updated Mar. 4, 2021) [hereinafter ICC Case Information Sheet].

[38] *Id.*

[39] *See generally* Trial Chamber Judgment, *supra* note 1, ¶¶ 129-77.

[40] *Id.* ¶ 135. Specifically, "there were contradictions and inconsistencies in the approach of the UN that created real problems for the OTP's investigators, and when assistance was sought the UN sometimes declined or imposed excessive constraints." *Id.* ¶ 135.

potential war criminals—the documents they produced were "more akin to general journalism than a legal investigation."[41]

One major issue affecting investigators' ability to collect evidence was security.[42] Armed militias were hostile to the ICC investigators' presence in Bunia.[43] Armed groups blocked the routes between Bunia and other towns, and the sound of gunfire was commonplace during the investigators' missions.[44] Because "any foreigner . . . was assumed to be from the ICC," investigators tried to hide the fact that they were conducting investigations.[45] Investigators were frequently at risk of attacks or abduction.[46] Witnesses were also placed at risk for working with investigators.[47] For security purposes, the ICC developed a "very specific and rigorous policy for investigators and witnesses—which slowed down the work of the OTP—because the priority was their security."[48] In order to avoid tipping off hostile political and military leaders in the region, investigators did not typically contact the families of witnesses—nor did they visit the schools that the children allegedly attended or try to acquire school records—despite the fact that these decisions slowed the investigative process.[49]

Investigators began interviewing witnesses in Bunia in 2005.[50] Investigators were responsible for traveling to various locations, identifying witnesses, and collecting statements.[51] These statements were provided to analysts, who determined whether the individuals should become testifying witnesses.[52] Once witnesses were identified, they worked with intermediaries who lived in the region in order to develop their testimony.[53]

Due to security concerns,[54] difficulty determining the ages of potential witnesses,[55] and challenges working with intermediaries in the field,[56] the investigation took two years to complete. Following the

---

[41] *See id.* ¶¶ 129-31.
[42] *See id.* ¶¶ 151-68.
[43] *Id.* ¶¶ 151-53.
[44] *Id.* For example, during one investigator's "first visit to Bunia, he heard gunfire from AK-47s in the neighbourhood of Mudzipela; indeed, every evening during the course of that mission he was aware of the sound of shooting." *Id.* ¶ 151.
[45] Trial Chamber Judgment, *supra* note 1, ¶ 154.
[46] *Id.* ¶ 155.
[47] *Id.* ¶ 156.
[48] *Id.* ¶ 156.
[49] *Id.* ¶¶ 160-61. This information about schooling and family life could also have helped investigators to determine children's ages.
[50] *Id.* ¶ 148.
[51] Trial Chamber Judgment, *supra* note 1, ¶ 148.
[52] *Id.* ¶¶ 149-50.
[53] *Id.* ¶¶ 190-91 To protect intermediaries' safety and to preserve their objectivity, investigators provided intermediaries with as little information about the case as possible. *Id.* ¶ 183.
[54] *See id.* ¶¶ 151-68.
[55] *See id.* ¶¶ 169-77
[56] *Id.* ¶¶ 183-97. Specifically,

investigation, on January 13, 2006, the Prosecutor applied for an arrest warrant for Lubanga.[57] On March 17, 2006, the DRC surrendered Lubanga, and he was transferred from the DRC to the ICC Detention Centre at The Hague.[58] On March 20, 2006, Lubanga made his initial court appearance.[59]

B. Charges Against Lubanga

Following multiple pretrial conferences,[60] the Pretrial Chamber issued its Decision on the Confirmation of Charges[61] on January 29, 2007.[62] It confirmed that there was sufficient evidence to establish substantial grounds to believe that both:

> Thomas Lubanga Dyilo is responsible, as co-perpetrator, for the charges of enlisting and conscripting children under the age of fifteen years into the FPLC and using them to participate actively in hostilities within the meaning of articles 8(2)(b)(xxvi) and 25(iii)(a) of the Statute from early September 2002 to 2 June 2003,[63]

and,

> [t]he fundamental question raised by the defense . . . is whether, during the investigations leading to this trial, four of the intermediaries employed by the prosecution suborned the witnesses they dealt with, when identifying or contacting these individuals or putting them in touch with the investigators, and whilst carrying out risk assessments. It is suggested, *inter alia*, that if this possibility is established, then any witnesses the intermediaries had dealings with should not be relied on. Indeed, it is argued that if this impropriety is substantively made out, the reliability of the prosecution's contentions in this case as a whole will be called into question.

Id. ¶ 178.

[57] ICC Case Information Sheet, *supra* note 37.

[58] *Id.*

[59] *Id.*

[60] One important ruling by the Pretrial Chamber regarded "witness-proofing," the practice of preparing witnesses before trial. Ruben Karemaker et al., *Witness Proofing in International Criminal Tribunals*, 21 LEIDEN J. INT'L L. 683, 687-89 (2008) (citing Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-679, Decision on the Practices of Witness Familiarisation and Witness Proofing (Nov. 8, 2006)). The Pretrial Chamber determined that only representatives from the Victim and Witnesses Unit, rather than the Prosecution, could prepare witnesses. *See id.* The term "witness proofing" was formally established by the Trial Chamber the following year. *See* Prosecutor v. Lubanga Dyilo, Decision Regarding the Practices Used to Prepare and Familiarise Witnesses for Giving Testimony at Trial, ICC-01/04-01/06-1049 (Nov. 30, 2007).

[61] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-803, Decision on the Confirmation of Charges, ¶ 410 (Jan. 29, 2007).

[62] The Prosecution decided not to charge sexual-based or gender crimes. *See* K'Shaani O. Smith, Prosecutor v. Lubanga*: How the International Criminal Court Failed the Women and Girls of the Congo*, 54 HOW. L. J. 467, 468 (2011).

[63] Trial Chamber Judgment, *supra* note 1, ¶ 1 (quoting Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-803-tEN, Decision on the Confirmation of Charges, at 156/157 (Jan. 29, 2007)). Art. 8(2)(b) refers to war crimes of an "international character." *See* Rome Statute, *supra* note 5, at art. 8(2)(b).

> Thomas Lubanga Dyilo is responsible, as co-perpetrator, for the charges of enlisting and conscripting children under the age of fifteen years into the FPLC and using them to participate actively in hostilities within the meaning of article 8(2)(e)(vii) of the Statute from 2 June to 13 August 2003.[64]

The first Trial Chamber status conference was held on September 4, 2007.[65] On June 13, 2008, the Trial Chamber stayed the proceedings because the Prosecutor failed to disclose potentially exculpatory evidence to the Defense.[66] The stay of proceedings was lifted on November 18, 2008.[67]

The trial commenced on January 26, 2009.[68] However, the Trial Chamber issued a second stay of proceedings on July 8, 2010 due to the Prosecution's non-compliance with a disclosure order regarding the name of one of the Intermediaries.[69] The trial recommenced in October 2010.[70]

C. Evaluation of Evidence

Sixty-seven witnesses testified over the course of 204 days of hearings.[71] Thirty-six witnesses[72]—including three experts—testified for the Prosecution.[73] Twenty-four witnesses testified for the Defense.[74] The Trial Chamber called four additional experts.[75] Overall, 1373 items of evidence were submitted—368 from the Prosecution, 992 from the Defense, and 13 from the legal representatives for the witnesses.[76] Both the Prosecution and the Defense introduced oral, written, and audio-visual testimony at trial.[77] This included oral testimony from witnesses who appeared either in person or via video link, two sworn depositions, and multiple written statements.[78]

---

[64] Trial Chamber Judgment, *supra* note 1, ¶ 1 (quoting Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-803-tEN, Decision on the Confirmation of Charges, at 157/157 (Jan. 29, 2007)). Art. 8(2)(e) refers to war crimes "not of an international character." *See* Rome Statute, *supra* note 5, at art. 8(2)(e).

[65] Trial Chamber Judgment, *supra* note 1, ¶ 10.

[66] *Id.*

[67] *Id.*

[68] *Id.* ¶ 10.

[69] *Id.*

[70] Trial Chamber Judgment, *supra* note 1, ¶ 10.

[71] *Id.* ¶ 11.

[72] Three victims were also called as witnesses. *Id.*

[73] *Id.*

[74] *Id.* ¶ 11.

[75] Trial Chamber Judgment, *supra* note 1, ¶ 11. These experts were Ms. Elisabeth Schauer, Mr. Roberto Garreton, Ms. Radhika Coomaraswamy, and Professor Kambayi Bwatshia. *Id.* at 14/593 n.29. One expert was a psychologist: she provided "expert testimony on the impact of a child having been a soldier and the effect of trauma on memory." *Id.* ¶ 105.

[76] *Id.* ¶ 11. Furthermore, the Chamber delivered 275 written decisions and orders, as well as 347 oral decisions, over the lifetime of the case. *Id.*

[77] *Id.* ¶ 93.

[78] *Id.*

In addition, "documents and other materials such as transcripts of interviews, videos, the records from a variety of organizations, letters, photographs, and maps were either introduced during the oral evidence of witnesses or by counsel."[79] The Trial Chamber admitted that it could not review all of the evidence in a timely fashion.[80] Therefore, the parties were instructed to flag evidence they considered "to have relevance and importance" and to provide short explanations of the key points made in relation to the evidence.[81] Four main issues arose from the Trial Chamber's evaluation of the evidence in *Lubanga*: the evidentiary standard, challenges to the credibility of intermediaries, difficulties determining witnesses' ages and credibility, and testimonial deficiencies.

i. Evidentiary Standards

First, the Trial Chamber fully considered the standard for evaluating evidence presented by both the Prosecution and the Defense. In order to evaluate oral testimony, the Trial Chamber:

> [c]onsidered the entirety of the witness's account; the manner in which he or she gave evidence; the plausibility of the testimony; and the extent to which it was consistent, including as regards other evidence in the case. The Chamber has assessed whether the witness's evidence conflicted with prior statements he or she has made, insofar as the relevant portion of the prior statement is in evidence. In each instance the Chamber has evaluated the extent and seriousness of the inconsistency and its impact on the overall reliability of the witness.[82]

The Trial Chamber made reasonable allowances for instances of "imprecision, implausibility or inconsistency," recognizing that memory fades over time (the events occurred between 2002 and 2003) and that witnesses who were under 15 years of age at the time of the events, or who suffered trauma, may "have had particular difficulty in providing a coherent, complete and logical account."[83]

Finally, the Trial Chamber "[c]onsidered the individual circumstances of each witness, including his or her relationship to the accused, age, vulnerability, any involvement in the events under consideration, the risk of self-incrimination, possible prejudice for or against the accused and motives for telling the truth or providing false testimony."[84]

---

[79] *Id.*
[80] Trial Chamber Judgment, *supra* note 1, ¶ 95.
[81] *Id.*
[82] *Id.* ¶ 102.
[83] *Id.* ¶ 103.
[84] *Id.* ¶ 106.

The Trial Chamber evaluated non-oral evidence on a case-by-case basis, based on "the nature and circumstances of the particular evidence," because the "Rome Statute provides the Chamber with a considerable degree of flexibility."[85] For documents, the Trial Chamber considered the document's author (if known), his or her role in the events, and the document's chain of custody.[86] The Trial Chamber evaluated expert witnesses based on competence in the field of expertise, methodologies used for data analysis, and the "general reliability" of the evidence.[87] The Trial Chamber also addressed the issues of "interpretation and translation."[88] Because testimony was presented in many different languages, the Trial Chamber conceded that this problem needed to be addressed on several occasions, even though no complaints about this issue were raised in the parties' final submissions.[89] Furthermore, the Trial Chamber considered the challenge of interpreting certain words, including locations and individuals' names.[90] The Trial Chamber utilized "protective measures" to protect witnesses' identities and to ensure their safety.[91]

ii. Intermediaries[92]

While the Defense challenged the credibility of many of the Prosecution's intermediaries[93] and the witnesses with whom they came in contact,[94] the Trial Chamber indicated that these individuals could be credible, but that the Trial Chamber needed to be persuaded beyond a reasonable doubt.[95] Specifically,

> with many of the witnesses . . . who came into contact with the intermediaries, the Chamber has recognized that they may well have given a truthful account as to elements of their past, including their involvement with the military, whilst at the same time—at least potentially—lying about particular crucial details, such as their identity, age, the dates of their military training and service, or the groups

[85] Trial Chamber Judgment, *supra* note 1, ¶¶ 107-08.
[86] *Id.* ¶ 109.
[87] *Id.* ¶ 112.
[88] *Id.* ¶ 113.
[89] *Id.*
[90] Trial Chamber Judgment, *supra* note 1, ¶ 114.
[91] *Id.* ¶¶ 115-17.
[92] *See generally* Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-2434, Redacted Decision on Intermediaries (May 31, 2010).
[93] Intermediaries worked with witnesses in the field, where they "assisted in identifying witnesses and they facilitated contact between the witnesses and the investigators. They helped with health problems, issues relating to threats and any lack of understanding on relevant issues." Trial Chamber Judgment, *supra* note 1, ¶ 190. In addition, they "assisted by contributing to the evaluation of the security situation." *Id.* ¶ 193.
[94] *Id.* ¶ 178.
[95] *Id.* ¶ 180.

> they were involved with. As regards this aspect of the case, the Chamber needs to be persuaded beyond a reasonable doubt that the alleged former child soldiers have given an accurate account on the issues that are relevant to this trial (*viz.* whether they were below 15 at the time they were conscripted, enlisted or used to participate actively in hostilities and the circumstances of their alleged involvement with the UPC).[96]

Neither the Prosecution nor the Defense intermediaries were provided with substantive information about the case.[97] They were unpaid, although their travel expenses were reimbursed.[98] Furthermore, neither the Prosecution nor the Defense witnesses were paid to answer questions, but their travel, lodging, and meal expenses were generally reimbursed.[99]

The Trial Chamber assessed the credibility of four intermediaries who the Defense alleged were unreliable, as well as the witnesses with whom they had contact.[100]

> In order to assess the role played by . . . each intermediary . . . and to determine whether the evidence given by the witnesses they had contacts with is reliable, the Chamber . . . considered each intermediary's involvement with the OTP and the relevant witnesses, as well as the particular evidence given by those witnesses.[101]

For example, two of Intermediary 143's four witnesses, P-0007 and P-0008,[102] were determined to be unreliable because of

> weaknesses and contradictions in their evidence (particularly as to their ages and true identities) along with the evidence of D-0012 undermine the reliability of their testimony. The difficulties with their accounts are not satisfactorily or sufficiently explained by fears for their safety or that of their family.[103]

After reviewing all four of Intermediary 143's witnesses, the Trial Chamber determined that none of them were credible.[104] The Trial Chamber concluded that "it is likely that as the common point of contact [Intermediary 143] persuaded, encouraged or assisted some or all of them to give false

---

[96] *Id.*
[97] *Id.* ¶ 183.
[98] *Id.* ¶ 198.
[99] Trial Chamber Judgment, *supra* note 1, ¶ 202.
[100] There were concerns that some intermediaries had coached witnesses to lie. *Id.* ¶ 180. The Chamber considered this when making credibility determinations. *Id.*
[101] *Id.* ¶ 207.
[102] "P" refers to Prosecution witnesses, and "D" refers to Defense witnesses.
[103] Trial Chamber Judgment, *supra* note 1, ¶ 247.
[104] *Id.* ¶¶ 208-21.

testimony."[105] The Trial Chamber proceeded with this method of evaluation for Intermediaries P-0316, P-0321, and P-0031, and it ultimately excluded several of the witnesses with whom they worked. The Trial Chamber determined that several of Intermediary 0321's witnesses were unreliable and that there was a distinct possibility that they were "encouraged and assisted by P-0321 to give false evidence."[106] However, Intermediary 0031's witnesses *were* deemed reliable, although the Trial Chamber recognized that their testimony should be carefully evaluated.[107]

iii. Age Assessments and Determinations of Witness Credibility

One major challenge facing the OTP in *Lubanga* was determining the children's ages at the time of the crimes.[108] Because the children did not carry identification, nor did the FPLC keep records,[109] investigators relied on forensic experts and doctors[110] to approximate the children's ages using techniques such as x-rays and physical examinations.[111]

The Trial Chamber considered a variety of factors to determine children's ages at the time of the events. In addition to the three experts called by the Prosecution and the four additional experts called by the Trial Chamber,[112] the Trial Chamber heard evidence from many non-expert witnesses. Age assessments were often "based on the individual's physical appearance, including by way of comparison with other children; the individual's general physical development (e.g. whether a girl had developed breasts, and factors such as height and voice); and his or her overall behavior."[113] In addition, the Prosecution provided several video excerpts to show that some of the child soldiers were "visibly" under age 15.[114] Investigators occasionally visited schools in the DRC to attempt to verify children's ages and identities.[115] However, this presented a security risk for both the investigators (because the FPLC, which occupied the region, was extremely hostile to the ICC investigators) and for the children (because

[105] *Id.* ¶ 291.
[106] *Id.* ¶ 449.
[107] *Id.* ¶¶ 476-77.
[108] *Id.* ¶¶ 169-77.
[109] Trial Chamber Judgment, *supra* note 1, ¶¶ 649-50. In fact, identification and documentation were uncommon in the DRC. *Id.*
[110] *Id.* ¶¶ 169-77. One doctor informed the investigators that five or six children were under age 15 because children in the community could not be baptized before a certain age. *Id.* ¶ 171.
[111] *Id.* ¶¶ 169-77.
[112] The Defense did not offer expert testimony. *Id.* ¶ 641. However, the Trial Chamber Judgment did not provide a reason for this decision.
[113] *Id.* ¶ 641.
[114] *Id.* ¶ 644.
[115] Trial Chamber Judgment, *supra* note 1, ¶ 644.

investigatory work would tip off the FPLC, and the FPLC might retaliate against the children or their families).[116]

iv. Testimonial Deficiencies

Witnesses exhibited a variety of testimonial deficiencies that raised potential doubts about their credibility at trial. Witnesses struggled to understand compound questions and basic terminology.[117] They had trouble identifying and estimating dates and ages,[118] durations,[119] distances,[120] numbers,[121] and other details about both the crimes alleged and the investigation.[122] Furthermore, there were inconsistencies between witnesses' pretrial statements and trial testimony,[123] as well as some evidence of perjury.[124]

D. Elements of the Crimes Charged: Article 8

In order to convict Lubanga as a co-perpetrator of the crime of "conscripting and enlisting children below the age of 15" under either Art. 8(2)(b)(xxvi)[125] or Art. 8(2)(e)(vii),[126] the Prosecutor needed to establish several elements.[127] First, that the FPLC engaged in an armed conflict (of either international or non-international character).[128] Then, that the crime fit the elements of either of these two provisions of Art. 8(2).[129] After the crime of conscription and enlistment of children under age 15 in an international or

[116] *Id.* ¶¶ 151-68.

[117] Trial Transcript at 10-12, *Lubanga* (Feb. 23, 2009), https://www.icc-cpi.int/Transcripts/CR2012_05409.PDF.

[118] Trial Transcript at 10-12, 23, *Lubanga* (Feb. 20, 2009), https://www.icc-cpi.int/Transcripts/CR2012_05184.PDF; Trial Transcript at 72, 77, *Lubanga* (Feb. 23, 2009); Trial Transcript at 7, *Lubanga* (Feb. 27, 2009), https://www.icc-cpi.int/Transcripts/CR2011_01442.PDF.

[119] Trial Transcript at 28, 38, 43-44, 46, *Lubanga* (Feb. 20, 2009); Trial Transcript at 66, 77, *Lubanga* (Feb. 23, 2009); Trial Transcript at 52, *Lubanga* (Mar. 6, 2009), https://www.icc-cpi.int/Transcripts/CR2012_04270.PDF.

[120] Trial Transcript at 65, *Lubanga*, (Feb. 23, 2009); Trial Transcript at 22-23, *Lubanga* (Mar. 4, 2009), https://www.icc-cpi.int/Transcripts/CR2012_04208.PDF.

[121] Trial Transcript at 12, 50, *Lubanga* (Feb. 20, 2009); Trial Transcript at 4, *Lubanga* (Feb. 23, 2009).

[122] Trial Transcript at 16, 26-27, 42, 45, *Lubanga* (Feb. 20, 2009); Trial Transcript at 76-77, *Lubanga*, (Feb. 23, 2009).

[123] Trial Transcript at 5-6, *Lubanga* (Feb. 27, 2009); Trial Transcript at 7-16, 18, 19, 30-32, 38-40, 49, 56-59, *Lubanga* (Mar. 4, 2009).

[124] Trial Transcript at 39-42, *Lubanga* (Jan. 28, 2009), https://www.icc-cpi.int/Transcripts/CR2012_04208.PDF.

[125] Rome Statute, *supra* note 5, at art. 8(2)(b)(xxvi). The war crime under this statute is an international armed conflict.

[126] Rome Statute, *supra* note 5, at art. 8(2)(e)(vii). The war crime under this statute is a conflict not of an international character.

[127] Trial Chamber Judgment, *supra* note 1, ¶¶ 503-04.

[128] *Id.*

[129] *Id.*

non-international armed conflict was established, it was also necessary to establish that Lubanga was individually criminally responsible for this crime.[130] This required establishing the "mental element" in Art. 30 of the Statute—specifically, that Lubanga acted with the intent and knowledge to perpetrate this crime.[131]

i. Armed Conflict and Its Nature[132]

To convict Lubanga under Article 8, the Prosecution first needed to establish that the FPLC engaged in an armed conflict. The relevant provisions of Article 8 of the Rome Statute[133] are as follows:

> i. The Court shall have jurisdiction in respect of war crimes in particular when committed as part of a plan or policy or as part of a large-scale commission of such crimes.
>
> ii. For the purposes of this Statute, 'war crimes' means:
>
> > b) Other serious violations of the laws and customs applicable in *international armed conflict*, within the established framework of international law [. . .]
> > e) Other serious violations of the laws and customs applicable in armed conflicts *not of an international character*, within the established framework of international law [. . .][134]

Furthermore, Art. 8(2)(f) of the Statute provides:[135]

> Paragraph 2(e) applies to armed conflicts not of an international character and thus does not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence or other acts of a similar nature. It applies to armed conflicts that take place in the territory of a State when there is protracted armed conflict between governmental authorities and organized armed groups or between such groups.[136]

---

[130] *Id.* ¶¶ 568-69.
[131] *Id.*
[132] *Id.* ¶¶ 503-04.
[133] Rome Statute, *supra* note 5, at art. 8.
[134] *Id.* at art. 8(1)-(2) (emphasis added).
[135] *Id.* at art. 8(2)(f); Trial Chamber Judgment, *supra* note 1, ¶ 534.
[136] Furthermore,

> Common Article 3 to the Geneva Conventions of 12 August 1949 provides: "In the case of an armed conflict not of an international character occurring in the territory of one of the High Contracting parties, […]"; Article 1(1) of Additional Protocol II reads: "This Protocol, which develops and supplements Article 3

In *Lubanga*, the Prosecution established beyond a reasonable doubt that during the time frame at issue, the FPLC participated in several simultaneous armed conflicts within Ituri and the surrounding areas within the DRC, some of which involved "protracted violence."[137] Furthermore, the conflict with other rebel groups was contained within the DRC, meaning that the conflict was non-international in character. Therefore, Art. 8(2)(e)(vii) was the applicable provision of the Statute.[138]

ii. Conscription and Enlistment of Children under the Age of 15 or Using them to Participate Actively in Hostilities (Art. 8(2)(e)(vii) of the Statute)[139]

After establishing that the FPLC was engaged in an armed conflict of a non-international character during this time period, it was necessary to proceed to the elements of conscription and enlistment of child soldiers and the corresponding Elements of Crimes.[140] Art. 8(2)(e)(vii)[141] reads:

> 2. [. . .]
>
> (e) Other serious violations of the laws and customs applicable in armed conflicts not of an international character, within the established framework of international law, namely, any of the following acts:

---

common to the Geneva Conventions of 12 August 1949 without modifying its existing conditions of application, shall apply to all armed conflicts which are not covered by Article 1 of the Protocol Additional to the Geneva Conventions of 12 August 1949, and relating to the Protection of Victims of International Armed Conflicts (Protocol I) and which take place in the territory of a High Contracting Party between its armed forces and dissident armed forces or other organized armed groups which, under responsible command, exercise such control over a part of its territory as to enable them to carry out sustained and concerted military operations and to implement this Protocol." Article 1(2) of Additional Protocol II provides as follows: "This Protocol shall not apply to situations of internal disturbances and tensions, such as riots, isolated and sporadic acts of violence and other acts of a similar nature, as not being armed conflicts." Whereas Common Article 2 is limited to international armed conflicts between signatories, Common Article 3 affords minimal protection to organised armed groups involved in any conflict not of an international character.

Trial Chamber Judgment, *supra* note 1, at 242/592 n.1630 (citing GERHARD WERLE, PRINCIPLES OF INTERNATIONAL CRIMINAL LAW 366 n.981 (Asser Press 2d ed. 2009); Andrew J. Carswell, *Classifying the Conflict: A Soldier's Dilemma*, 91 INT'L REV. RED CROSS 143, 150 (2009); GARY D. SOLIS, THE LAW OF ARMED CONFLICT 157 (Cambridge Univ. Press 1st ed. 2010)).

[137] Trial Chamber Judgment, *supra* note 1, ¶¶ 543-50.

[138] *Id.* ¶¶ 565-66.

[139] *Id.* ¶¶ 568-69.

[140] *Id.* ¶¶ 568-71.

[141] The Rome Statute was the first treaty to classify this offense of conscription and enlistment of child soldiers as a war crime. *Id.* ¶ 569.

[. . .]

> (vii) Conscripting or enlisting children under the age of fifteen years into armed forces or groups or using them to participate actively in hostilities.[142]

Furthermore, the corresponding Elements of Crimes reads:

> The perpetrator conscripted or enlisted one or more persons into an armed force or group or used one or more persons to participate actively in hostilities.
>
> Such a person or persons were under the age of 15 years.
>
> The perpetrator knew of should have known that such person or persons were under the age of 15 years.
>
> The conduct took place in the context of and was associated with an armed conflict not of an international character.
>
> The perpetrator was aware of the factual circumstances that established the existence of an armed conflict. [143]

While neither the Statute, nor the Rules, nor the Elements of Crimes defines "conscripting or enlisting children under the age of 15 or using them to participate actively in hostilities," the SCSL has a nearly identical provision under Art. 4(c) of its Statute.[144] Therefore, the SCSL's case law is particularly instructive.

The Trial Chamber concluded that the FPLC engaged in widespread recruitment on both voluntary and forced bases between September 1, 2002 and August 13, 2003.[145] The Trial Chamber based its conclusion on both documentary evidence and witness testimony.[146] The Trial Chamber also admitted video evidence from one training camp that showed recruits "clearly" under age 15.[147] It was established that during this period, Lubanga and several other military leaders participated actively in "mobilization drives and recruitment campaigns that were directed at persuading Hema families to send their children to serve in the UPC/FPLC army."[148] Testimony

---

[142] *Id.*; Rome Statute, *supra* note 5, at art. 8(2)(e)(vii).

[143] Trial Chamber Judgment, *supra* note 1, ¶ 569.

[144] *Id.* ¶¶ 600-03.

[145] *Id.* ¶ 911.

[146] The Trial Chamber made the following evidentiary determinations, based on the evaluative criteria previously discussed: (1) logbooks from a "demobilization center" were unreliable, *id.* ¶¶ 733-40; (2) a letter from the National Secretary of Education to the G5 Commander of the FPLC (dated Feb. 12, 2003) referencing recruiting children under age 15, was reliable, *id.* ¶¶ 741-48; (3) a logbook of radio communications was unreliable, *id.* ¶¶ 749-52; and (4) a "monthly report" by a member of senior leadership was relevant to establish the "recruitment" aspect, but not to determine children's ages, *id.* ¶¶ 753-58.

[147] *Id.* ¶ 912.

[148] *Id.* ¶ 911.

further revealed that children in the camps "endured a harsh training regime" and that "they were subjected to a variety of severe punishments."[149] In addition, testimony revealed that children were deployed as soldiers in Bunia, Tchoia, Kasenyi, and Bogoro, and that they took part in fighting in Kobu, Songolo, and Mongbwalu.[150] Children were also used as bodyguards: in fact, video evidence revealed that children under age 15 served as bodyguards for Lubanga himself.[151]

iii. Individual Criminal Responsibility of Thomas Lubanga (Article 25(3)(a) of the Statute)[152]

After establishing that members of the FPLC committed the crimes of "conscripting or enlisting children under the age of 15, or using them to participate actively in hostilities," the Prosecution needed to establish that Lubanga was individually criminally responsible as a co-perpetrator.[153] Art. 25(3)(a) reads, in relevant part:

> *A.* The Court shall have jurisdiction over natural persons pursuant to this Statute.
> *B.* A person who commits a crime within the jurisdiction of the Court shall be individually responsible and liable for punishment in accordance with this Statute.
> *C.* In accordance with this Statute, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court if that person:
> a. Commits such a crime, whether as an individual, *jointly with another* or through another person, regardless of whether that other person is criminally responsible.[154]

The Prosecution also needed to establish the "mental element" of this crime under Article 30[155] of the Statute.[156] The Chamber concluded that, in order to

---

[149] Trial Chamber Judgment, *supra* note 1, ¶ 913.
[150] *Id.* ¶ 915.
[151] *Id.*
[152] *Id.* ¶ 917.
[153] *Id.* ¶¶ 917-18.
[154] *Id.* ¶ 917.
[155] Rome Statute, *supra* note 5, at art. 30.
[156] Trial Chamber Judgment, *supra* note 1, ¶¶ 974-75. Specifically,
> 1. Unless otherwise provided, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the court only if the material elements are committed with intent and knowledge.
> 2. For the purposes of this article, a person has intent where:
> a. In relation to conduct, that person means to engage in the conduct;
> b. In relation to a consequence, that person means to cause that consequence or is aware that it will occur in the ordinary course of events.

establish Lubanga's responsibility as a co-perpetrator, the Prosecution needed to prove that:

> (i) There was an agreement or common plan between the accused and at least one co-perpetrator that, once implemented, will result in the commission of the relevant crime in the ordinary course of events;
> (ii) The accused provided an essential contribution to the common plan that resulted in the commission of the relevant crime;
> (iii) The accused meant to conscript, enlist, or use children under the age of 15 to participate actively in hostilities or he was aware that by implementing the common plan, these consequences "will occur in the ordinary course of events;"
> (iv) The accused was aware that he provided an essential contribution to the implementation of the common plan; and
> (v) The accused was aware of the factual circumstances that established the existence of an armed conflict and the link between these circumstances and his conduct.[157]

The Trial Chamber concluded that all five elements had been proven beyond a reasonable doubt.[158] First, Lubanga and his co-perpetrators agreed to and participated in a common plan to create an army to secure control over Ituri, which "resulted, in the ordinary course of events, in the conscription and enlistment of boys and girls under the age of 15, and their use to participate actively in hostilities.[159] Second, Lubanga provided essential contributions to the common plan because he "exercised an overall coordinating role" over the FPLC's activities; he was "closely involved" in decision-making and recruitment policies; he gave speeches to recruit children under age 15; and he personally used bodyguards under age 15.[160] Finally, regarding elements (iii)-(v) above, Lubanga acted with the requisite intent and knowledge because:

> he was aware of the factual circumstances that established the existence of the armed conflict. Furthermore, he was

---

> 3. For the purposes of this article, 'knowledge' means awareness that a circumstance exists or a consequence will occur in the ordinary course of events. 'Know' and 'knowingly' shall be construed accordingly.

Id.

[157] *Id.* ¶ 1018.
[158] *Id.* ¶¶ 1351-57.
[159] *Id.* ¶ 1351.
[160] *Id.* ¶1356.

> aware of the nexus between those circumstances and his own conduct, which resulted in this enlistment, conscription and use of children below the age of 15 to participate actively in hostilities.[161]

E. Conviction, Sentencing, and Appeals

The trial concluded on August 26, 2011.[162] On March 14, 2012, Lubanga was convicted of "the crimes of conscripting and enlisting children under the age of fifteen years into the FPLC and using them to participate actively in hostilities within the meaning of Articles 8(2)(e)(vii) and 25(3)(a) of the Statute from early September 2002 to 13 August 2003."[163]

On July 10, 2012, Lubanga was sentenced to 14 years' imprisonment.[164] However, the time that Lubanga spent in ICC custody beginning in March 2006 was deducted from his sentence.[165] On December 1, 2014, the Appeals Chamber confirmed Lubanga's conviction and sentence.[166] On September 22, 2015, the Appeals Chamber denied Lubanga's motion for a sentence reduction.[167] The Appeals Chamber reexamined the motion on November 3, 2017 and once again rejected the motion for reduction of Lubanga's sentence.[168] On December 15, 2017, Trial Chamber II set the amount of Lubanga's reparations at 10 million USD.[169] Lubanga spent the rest of his sentence imprisoned in the DRC.[170]

---

[161] *Id.* ¶ 1357.

[162] *Id.* ¶ 11.

[163] *Id.* ¶ 1358. Furthermore, "[p]ursuant to Regulation 55 of the Regulations of the Court, the Chamber modifies the legal characterisation of the facts to the extent that the armed conflict relevant to the charges was non-international in character…." *Id.* ¶ 1359.

[164] Lubanga Decision on Sentence, *supra* note 9, ¶¶ 107-08.

[165] *Id.* ¶ 108.

[166] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-3121, Judgment on the Appeal of Mr. Thomas Lubanga Dyilo against His Conviction, ¶ 529 (Dec. 1, 2014).

[167] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-3173, Decision on the Review Concerning Reduction of Sentence of Mr. Thomas Lubanga Dyilo, ¶¶ 77-79 (Sept. 22, 2015).

[168] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-3375, Second Decision on the Review Concerning Reduction of Sentence of Mr. Thomas Lubanga Dyilo, ¶ 94-95 (Nov. 3, 2017).

[169] *See* Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-3379, Decision Setting the Size of the Reparations Award for which Thomas Lubanga Dyilo is Liable, ¶ 281 (Dec. 21, 2017) [hereinafter Lubanga Decision Setting Reparations]. This reparations award was placed in a Victim Compensation Fund to compensate 425 victims. *Id.* at ¶ 279. In total, 3.4 million USD in compensation was awarded to the victims (8000 USD per victim). *Id.* The Chamber awarded an additional 6.6 million USD. *Id.* at ¶ 280; *see also* News Wires, *DR Congo Ex-child Soldiers Awarded $10 Million in Damages*, FRANCE 24 (Dec. 16, 2017), https://www.france24.com/en/20171215-dr-congo-child-soldiers-awarded-10-million-dollars-compensation-lubanga-icc.

[170] *See generally* Lubanga Decision on Sentence, *supra* note 9.

F. Separate Opinions

Judge Adrian Fulford filed a separate opinion in the Trial Chamber Judgment in which he concurred with the Trial Chamber's judgment that Lubanga was guilty of conscripting and enlisting child soldiers under Art. 8(2)(e)(vii) of the Statute and that Lubanga was liable as a co-perpetrator under Art. 25(3)(a), according to the tests set out in Paragraphs 1013[171] and 1018[172] of the Judgment.[173] However, Judge Fulford argued that the Trial Chamber should have applied a "different, and arguably lesser, test" to establish Lubanga's liability under Art. 25(3), because the high standard established in Art. 25(a)(3) placed an "unnecessary and unfair burden on the prosecution."[174] Judge Fulford conceded that it would be unfair to Lubanga to retroactively apply a different standard.[175]

Judge Fulford disapproved of the "hierarchy of seriousness" through which the Trial Chamber distinguished between "principal" and "accessory" liability.[176] Specifically, the Trial Chamber distinguished between four degrees of liability within Art. 25(3): Art. 25(a)(3) (liability as a co-perpetrator, also referred to as the "control of the crime theory"),[177] and Arts. 25(3)(b-d), which represented lesser forms of liability that included ordering,

---

[171] "The Chamber is of the view that the prosecution must establish, as regards the mental element, that:

(i) the accused and at least one other perpetrator meant to conscript, enlist or use children under the age of 15 to participate actively in hostilities or they were aware that in implementing their common plan this consequence "will occur in the ordinary course of events"; and

(ii) the accused was aware that he provided an essential contribution to the implementation of the common plan..."

Trial Chamber Judgment, *supra* note 1, ¶ 1013.

[172] The Prosecution was required to prove five elements in order to establish Lubanga's liability as a co-perpetrator:

(i) there was an agreement or common plan between the accused and at least one other co-perpetrator that, once implemented, will result in the commission of the relevant crime in the ordinary course of events;

(ii) the accused provided an essential contribution to the common plan that resulted in the commission of the relevant crime;

(iii) the accused meant to conscript, enlist or use children under the age of 15 to participate actively in hostilities or he was aware that by implementing the common plan these consequences "will occur in the ordinary course of events";

(iv) the accused was aware that he provided an essential contribution to the implementation of the common plan; and

(v) the accused was aware of the factual circumstances that established the existence of an armed conflict and the link between these circumstances and his conduct.

Id. ¶ 1018.

[173] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-2842, Separate Opinion of Judge Fulford, ¶¶ 1-21 (Mar. 14, 2012) [hereinafter Judge Fulford Separate Opinion].

[174] *Id.* ¶¶ 2-3.

[175] *Id.* ¶ 2.

[176] *Id.* ¶ 9.

[177] *Id.* ¶¶ 5-6.

soliciting, or inducing (Art. 25(3)(b)), accessory liability (Art. 25(3)(c)), and participation within a group (Art. 25(3)(d)).[178] Judge Fulford advocated instead for a "plain reading" of Art. 25(3)[179] in which "individuals who are involved *indirectly*[180] can be prosecuted as co-perpetrators."[181]

Judge Odio Benito filed a dissenting opinion in the Trial Chamber Judgment in which she agreed with the Trial Chamber's final decision regarding Lubanga's individual criminal responsibility for the crimes of conscripting and enlisting children under the age of 15 but disagreed with three particular aspects of the judgment.[182] First, Judge Benito disagreed with the "legal definition of the crimes of enlistment, conscription and use of children under the age of 15 to actively participate in the hostilities."[183] Specifically, Judge Benito argued that the definition should be broadened to include "any type of armed group or force, regardless of the nature of the armed conflict in which it occurs."[184] Judge Benito highlighted the severity of sexual violence and noted that gender-based and sexual violence are "distinct and separate crimes that could have been evaluated separately . . . if the Prosecutor would have presented charges."[185]

Second, Judge Benito disagreed with the Trial Chamber regarding the "dual status victims/witnesses." Specifically, Judge Benito argued that, while several of the dual status victims/witnesses' testimonies should not be used to determine Lubanga's criminal responsibility, these victims/witnesses should still have been permitted to participate in the trial as victims.[186]

---

[178] *Id.* ¶ 8.

[179] Judge Fulford Separate Opinion, *supra* note 173, ¶ 14. Specifically,

> [i]n accordance with this Statute, a person shall be criminally responsible and liable for punishment for a crime within the jurisdiction of the Court if that person . . . [c]ommits such a crime, whether as an individual, jointly with another or through another person, regardless of whether that other person is criminally responsible...

Id.

[180] *Id.* (emphasis added).

[181] *Id.* ¶ 12.

[182] Prosecutor v. Lubanga Dyilo, ICC-01/04-01/06-2842, Separate and Dissenting Opinion of Judge Benito, ¶¶ 1-43 (Mar. 14, 2012) [hereinafter Separate and Dissenting Opinion of Judge Benito].

[183] *Id.* ¶¶ 2-21.

[184] *Id.* ¶ 14.

[185] *Id.* ¶ 20. Specifically,

> [i]f the war crimes considered in this case are directed at securing [children's] physical and psychological well being, then we must recognize sexual violence as a failure to afford this protection and sexual violence as acts embedded in the enlisting, conscription and use of children under 15 in hostilities. It is discriminatory to exclude sexual violence which shows a clear gender differential impact from being a bodyguard or porter which is mainly a task given to young boys.

Id. ¶ 21.

[186] *Id.* ¶¶ 22-35. Specifically,

Finally, Judge Benito argued that the Trial Chamber should have considered the evidentiary value of several additional pieces of video evidence.[187]

III. HISTORY OF CHILD SOLDIER PROSECUTIONS: THE SPECIAL COURT FOR SIERRA LEONE CASES

While *Lubanga* was the first child soldier case[188] prosecuted at the ICC, the Special Court for Sierra Leone ("SCSL")[189] convicted several individuals in the late 2000s of conscripting and enlisting child soldiers[190] in the three subsequent cases.[191] Both the Pretrial and Trial Chambers in *Lubanga* considered SCSL jurisprudence throughout the case.[192] The three cases that follow consider evidentiary issues, including concerns about testimonial discrepancies and inaccuracies, which ICC prosecutors later faced in *Lubanga*.[193] Because *Lubanga* presented an issue of first impression for the ICC, the SCSL cases are particularly instructive.[194]

> [t]hese witnesses . . . could explicably and logically have difficulties in recollecting events since the time elapsed between the events (2002-2003), the first interviews with OTP investigators (2005) and the actual trial (2009-2010). In fact, with such elapses of time it would be suspicious if the accounts would remain perfectly alike and unchanged. Memory is faulty. This is more the case for children and adults having suffered any traumatic events.

Id. ¶ 32.

[187] *Id.* ¶¶ 36-43.

[188] It has been postulated that "child soldiers are frequently used to commit war crimes and crimes against humanity, particularly because commanders find it easier to manipulate children to commit more audacious crimes than it is to convince adults." Belinda S.T Hlatshwayo, International Criminal Law and the African Girl Child Solider: Does the International Criminal Law Framework Provide Adequate Protection to the African Girl Child Soldier? (Mar. 12, 2017) (LLM dissertation, Univ. of Cape Town) (on file with the Univ. of Cape Town library) (citing DAVID M. ROSEN, ARMIES OF THE YOUNG: CHILD SOLDIERS IN WAR AND TERRORISM 9 (Rutgers Univ. Press 2005).

[189] The SCSL "was set up in 2002 as the result of a request to the United Nations in 2000 by the Government of Sierra Leone for 'a special court' to address serious crimes against civilians and UN peacekeepers committed during the country's decade-long (1991-2002) civil war." Residual Special Court for Sierra Leone, *supra* note 2. The Residual Special Court of Sierra Leone (RSCSL) was established in 2012. *Id.*

[190] One individual's conviction for conscripting and enlisting child soldiers was overturned on appeal: however, his convictions for other crimes were upheld on appeal. *See infra* note 191.

[191] *See* Prosecutor v. Fofana, SCSL-04-14-T-785, Judgement, ¶¶ 972-73 (Aug. 2, 2007) [hereinafter CDF Case]; Prosecutor v. Sesay, SCSL-04-15-T-1234, Judgement, ¶¶ 1747-48 (Mar. 2, 2009) [hereinafter RUF Case]; Prosecutor v. Brima, SCSL-04-16-T-613, Judgement, ¶¶ 727, 731 (June 20, 2007) [hereinafter AFRC Case].

[192] Trial Chamber Judgment, *supra* note 1, ¶ 603 ("[T]he wording of the provision criminalising the conscription, enlistment and use of children under the age of 15 within the Statute of the SCSL is identical to Article 8(e)(vii) of the Rome Statute, and they were self-evidently directed at the same objective. The SCSL's case law therefore potentially assists in the interpretation of the relevant provisions of the Rome Statute.").

[193] *See* CDF Case, *supra* note 191; RUF Case, *supra* note 191; AFRC Case, *supra* note 191.

[194] *See* JULIE MCBRIDE, THE WAR CRIME OF CHILD SOLDIER RECRUITMENT 147 (Asser Press 2014). Specifically,

The Rome Statute had not addressed the crime of "conscripting, enlisting children under the age of 15, or using them to participate actively in hostilities" prior to *Lubanga*. Therefore, the Chamber looked to the SCSL's analysis of child soldier cases prosecuted under Art. 4(c)[195] of the Statute of the SCSL.[196]

A. The Prosecutor v. Alex Tamba Brima, Ibrahim Bazzy Kamara and Santigie Borbor Kanu

The Prosecutor v. Alex Tamba Brima, Ibrahim Bazzy Kamara and Santigie Borbor Kanu ("the AFRC Case")[197] was the first case to successfully convict—and uphold on appeal—individuals for the crimes of conscripting and enlisting child soldiers. In the AFRC Case, three high-ranking military officials from the Armed Forces Revolutionary Council ("AFRC") were convicted of, among other crimes, "conscripting children under the age of 15 years into an armed group and/or using them to participate actively in hostilities . . . pursuant to Article 4(c) of the Statute."[198] All three were held individually criminally responsible pursuant to Art. 6(1)[199] of the Statute of the SCSL.

The AFRC Case tackled many of the issues that would later appear in *Lubanga* regarding the evaluation of evidence and the assessment of witness credibility.[200] In addressing discrepancies within a witness's multiple statements, the AFRC Trial Chamber applied the International Criminal

> [t]he Pre-Trial Chamber follows the reasoning of the Special Court on a number of critical issues, notably determining the means of recruitment—either enlistment or conscription—is ultimately irrelevant, and voluntariness is no defense. In tackling the definition of 'use' [of child soldiers], the Pre-Trial Chamber followed the Special Court's precedent and made a list of which activities constitute active participation in hostilities.

Id.

[195] Art. 4(c) of the Statute of the Special Court for Sierra Leone reads, "conscripting or enlisting children under the age of 15 years into armed forces or groups or using them to participate actively in hostilities." Statute of the Special Court for Sierra Leone art. 4(c), Jan. 16, 2002, 2178 U.N.T.S. 138.

[196] *Id.*

[197] This Article describes the AFRC Case in slightly more detail than the CDF and RUF Cases that follow because it was precedent-setting at the SCSL.

[198] AFRC Case, *supra* note 191, ¶¶ 2112-23.

[199] Art. 6(1) reads as follows: "A person who planned, instigated, ordered, committed or otherwise aided and abetted in the planning, preparation or execution of a crime referred to in articles 2 to 4 of the present Statute shall be individually responsible for the crime." Statute of the Special Court for Sierra Leone, *supra* note 195, at art. 6(1).

[200] *See generally* AFRC Case, *supra* note 191, including emotional responses, *id.* ¶¶ 110-13; names of locations, *id.* ¶ 115; witness self-interest and perjury incentives, *id.* ¶¶ 124-30; determining credibility of former child soldiers, *id.* ¶¶ 1252-61; and determining credibility of individuals allegedly harmed by former child soldiers, *id.* ¶¶ 1262-75.

Tribunal for the former Yugoslavia ("ICTY") Appeals Chamber's statement in *Kupreškić*:[201]

> The presence of inconsistencies in the evidence does not, *per se*, require a reasonable Trial Chamber to reject it as being unreliable. Similarly, factors such as the passage of time between the events and the testimony of the witness, the possible influence of third persons, discrepancies, or the existence of stressful conditions at the time the events took place do not automatically exclude the Trial Chamber from relying on the evidence.[202]

The AFRC Trial Chamber conceded that in-court testimony might evoke strong emotional responses from witnesses—including bringing them to tears.[203] It acknowledged that the trauma that victim-witnesses suffered might prevent them from providing a full account of their experiences or could affect their memories.[204] Furthermore, the Trial Chamber asserted that a witness's observations at the time of the events might be affected by terror or stress.[205] In addition, the Trial Chamber indicated that the passage of time (more than six years had passed since the crimes occurred) could affect the accuracy of witnesses' memories.[206] Also, interviews conducted in other languages and then translated for the Trial Chamber could pose communications confusion.[207]

The Trial Chamber noted that the appearance of a desire to exculpate oneself from crimes to which the individual was a party[208] by falsifying testimony (a "perjury incentive") did not automatically render the testimony unusable.[209] Finally, the Trial Chamber was not convinced by the Defense's argument that witnesses received "financial incentives" to testify—in fact, the "incentives" to which the Defense referred were medical, travel, food, and lodging reimbursement for individuals who testified that they had been forced to become child soldiers.[210] In sum, none of these factors was determinative; rather, the Trial Chamber evaluated each witness on a case-by-case basis.[211] The Trial Chamber did not treat minor discrepancies—such

---

[201] Prosecutor v. Kupreškić, Case No. IT-95-16-A, Appeal Judgement, ¶ 31 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 23, 2001).

[202] AFRC Case, *supra* note 191, ¶ 110 (citing Prosecutor v. Kupreškić, Case No. IT-95-16-A, Appeal Judgement, ¶ 31 (Int'l Crim. Trib. for the Former Yugoslavia Oct. 23, 2001)).

[203] *Id.* ¶ 111.

[204] *Id.*

[205] *Id.*

[206] *Id.* ¶ 112.

[207] *Id.*

[208] *See* Combs, *supra* note 16, at 116 ("Accomplice witness testimony may [seem] particularly reliable…because accomplice witnesses often [know] more than non-accomplice witnesses about the events in question, and specifically about the defendant's conduct.").

[209] AFRC Case, *supra* note 191, ¶ 125.

[210] *Id.* ¶¶ 126-30.

[211] *Id.* ¶ 111.

as names or locations[212]—as "discrediting their evidence where the essence of the incident had nevertheless been recounted in acceptable detail."[213]

The AFRC Trial Chamber was concerned with many types of evidentiary discrepancies. These included: witnesses' inability to determine their own ages;[214] remember dates;[215] estimate durations,[216] distances,[217] and numbers;[218] review two-dimensional representations, such as maps, graphs, and charts;[219] and understand court procedures.[220] The Trial Chamber was also concerned with linguistic miscommunication between international witnesses, judges, and attorneys. Witnesses did not always understand the terminology used in the attorneys' questioning.[221] Some witnesses struggled to answer compound, multi-part, or generally complex questions[222] during testimony.[223] In addition, the Trial Chamber was concerned with cultural and educational barriers. For example, many witnesses were illiterate or had received very little education.[224] In fact, one witness grew frustrated when he was repeatedly asked to spell names.[225] Finally, interpreters faced challenges in accurately translating testimony during the trial.[226]

---

[212] *Id.* ¶ 115.

[213] *Id.* ¶ 113.

[214] *See* Trial Transcript at 64-65, AFRC Case (July 5, 2005). For access to AFRC trial transcripts, visit *AFRC Transcripts*, RESIDUAL SPECIAL COURT FOR SIERRA LEONE, http://www.rscsl.org/AFRC_Transcripts.html (last visited Apr. 17, 2021).

[215] *See* Trial Transcript at 30, AFRC Case (July 25, 2005); Trial Transcript at 73-75, AFRC Case (Apr. 7, 2005).

[216] *See* Trial Transcript at 58-59, AFRC Case (Mar. 8, 2005); Trial Transcript at 112, AFRC Case (Apr. 7, 2005).

[217] *See* Trial Transcript at 31, AFRC Case (Mar. 8, 2005).

[218] *See* Trial Transcript at 107, AFRC Case (Apr. 7, 2005); Trial Transcript at 79, AFRC Case (June 27, 2005); Trial Transcript at 43, AFRC Case (Mar. 8, 2005).

[219] *See* Trial Transcript at 29, AFRC Case (July 25, 2005).

[220] *See* Trial Transcript at 50-52, AFRC Case (Apr. 6, 2005).

[221] *See* Trial Transcript at 67 (Apr. 7, 2005); Trial Transcript at 21-22, AFRC Case (Apr. 6, 2005); Trial Transcript at 109-11, AFRC Case (July 18, 2005).

[222] Even in Western countries, both child and adult witnesses may struggle to understand compound and multi-part questions. *See* COMBS, *supra* note 13, at 46-47 (citing LOUISE ELLISON, THE ADVERSARIAL PROCESS AND THE VULNERABLE WITNESS 95 (Oxford Univ. Press 2002); Ingrid M. Cordon et al., *Children in Court*, *in* ADVERSARIAL VERSUS INQUISITORIAL JUSTICE: PSYCHOLOGICAL PERSPECTIVES ON CRIMINAL JUSTICE SYSTEMS, 167, 171 (Peter J. van Koppen & Steven D. Penrod eds., 2003)).

[223] *See* Trial Transcript at 107-08, AFRC Case (June 30, 2005); Trial Transcript at 35-36, AFRC Case (July 1, 2005); Trial Transcript at 108-09, AFRC Case (July 18, 2005).

[224] *See* Trial Transcript at 29, AFRC Case (July 25, 2005) (witness could not read or write); Trial Transcript at 3, 12, 45, 58, 77, AFRC Case (Sept. 27, 2005) (witness had trouble spelling). In fact, out of the forty-five witnesses in the AFRC Case for which education and literacy data are available, twenty-one witnesses (forty-seven percent) "were illiterate and/or had never attended school." COMBS, *supra* note 13, at 64.

[225] Trial Transcript at 11, 58, 77, AFRC Case (Sept. 27, 2005).

[226] Trial Transcript at 104, AFRC Case (Apr. 7, 2005).

In evaluating the testimonial evidence,[227] the Trial Chamber heard from expert witnesses,[228] former child soldiers,[229] and individuals who had been harmed or victimized by former child soldiers.[230] The Trial Chamber determined that two witnesses were credible (TF1-157 and TF1-158)[231] and three were not.[232] In its assessment of TF1-157, the Trial Chamber found the precision with which the individual described both (1) his journey from town to town during his time as a child soldier, and (2) the atrocities he witnessed committed against his family members, as well as the fact that he did not appear shaken on cross-examination, to be compelling.[233] TF1-158, the brother of TF1-157, was also found to be credible, not only because of the precise nature with which he described the events, and the fact that he did not appear shaken on cross-examination, but also because his account of his separate experiences was distinct from his brother's—suggesting that they had not coordinated their stories.[234] The Trial Chamber considered testimonial discrepancies, communications challenges, and cultural and educational barriers, but it ultimately determined that these were overshadowed by the aforementioned compelling factors.[235]

For the three witnesses who were determined not to be credible, the Trial Chamber indicated that their stories could not be corroborated with any other testimony.[236] After the Trial Chamber enumerated many factors that it would consider in assessing witness credibility, the Trial Chamber indicated that each witness's appearance on cross-examination was particularly important.[237] The Trial Chamber determined that the testimonies of multiple witnesses who alleged that they had been harmed by child soldiers were not credible because one individual could not remember the child soldiers' ages; one individual's descriptions of various locations were too vague; and in several cases, the Trial Chamber could not find evidence, based on their testimonies, linking the information to the Accused.[238] Despite the fact that some testimony was ultimately excluded, the Trial Chamber stated that "a significant amount of evidence has been adduced by both Prosecution and Defense witnesses in respect of each of these crimes over the course of a lengthy trial."[239]

The AFRC Case is instructive because it applied Art. 4(c) of the Statute of the SCSL which, as previously discussed, is nearly identical to Art.

---

[227] The Trial Chamber in the AFRC Case also considered documentary evidence.
[228] AFRC Case, *supra* note 191, ¶¶ 1248-51.
[229] *Id.* ¶¶ 1252-61.
[230] *Id.* ¶¶ 1262-75.
[231] *Id.* ¶ 1252.
[232] *Id.* ¶ 1262.
[233] *Id.* ¶¶ 1252-55.
[234] AFRC Case, *supra* note 191, ¶¶ 1256-58.
[235] *Id.* ¶¶ 1276-78.
[236] *Id.* ¶¶ 1259-61.
[237] *Id.* ¶¶ 1262-75.
[238] *Id.* ¶¶ 1262-75.
[239] *Id.* ¶ 41.

8(2)(e)(vii) of the Rome Statute. Furthermore, the Trial Chamber highlighted many factors that it considered in evaluating evidence that would ultimately serve to convict three individuals of, among other crimes, conscripting and enlisting child soldiers. The two SCSL cases that followed the AFRC Case also provide important context for the *Lubanga* case.

B. The Prosecutor v. Sam Hinga Norman, Moinina Fofana and Allieu Kondewa

Two months after the AFRC Case was decided, in *The Prosecutor v. Sam Hinga Norman, Moinina Fofana and Allieu Kondewa* ("CDF Case"),[240] the SCSL Trial Chamber found Moinina Fofana and Allieu Kondewa,[241] two leaders of the Civil Defence Forces ("CDF"), guilty of multiple crimes including murder, cruel treatment, and pillage.[242] The crime of conscripting and enlisting child soldiers (Count 8) was analyzed: however, the Trial Chamber acquitted Fofana on Count 8, and Kondewa's conviction on Count 8 was overturned on appeal.[243]

As in both the AFRC Case and *Lubanga*, the Trial Chamber acknowledged that "[m]inor inconsistencies in testimony do not necessarily discredit a witness. The events in question took place several years ago and, due to the nature of memory, some details will be confused, and some will be forgotten."[244] Furthermore, witnesses' testimony need not be identical to prior statements: for example, oral testimony at trial involves more comprehensive questions and questions not previously asked.[245]

The Trial Chamber convicted Kondewa on Count 8 pursuant to Art. 6(3)[246] of the Statute of the SCSL based on the testimony of a single child witness, TF2-021,[247] despite inconsistencies between TF2-021's testimony and that of other witnesses.[248] In addition to this child witness's testimony,

---

[240] *See* CDF Case, *supra* note 191.

[241] Norman died in 2007, after the close of witness testimony but before judgment. Nick Tattersall, *S.Leone War Crimes Indictee Hinga Norman Dies*, REUTERS (Feb. 22, 2007, 9:22 AM), https://www.reuters.com/article/us-leone-warcrimes-norman/s-leone-war-crimes-indictee-hinga-norman-dies-idUSL2252331020070222.

[242] *See* CDF Case, *supra* note 191, ¶¶ 975-78. Notably, the Appeals Chamber held, in a decision on a preliminary motion, that conscripting and enlisting soldiers was a violation of international humanitarian law at the time of the crime. *See generally* Prosecutor v. Norman, SCSL-2004-14-AR72(E), Decision on Preliminary Motion Based on Lack of Jurisdiction (Child Recruitment), ¶ 54 (May 31, 2004).

[243] Prosecutor v. Fofana, SCSL-04-14-A, App. Chamber Judgment, at 134/246 (May 28, 2008). Furthermore, the Appeals Chamber overturned convictions for both Fofana and Kondewa on Count 7 (collective punishments). *Id.*

[244] CDF Case, *supra* note 191, ¶ 262.

[245] *Id.* ¶ 263.

[246] The Trial Chamber indicated that, because it found Kondewa guilty pursuant to Art. 6(3), it was not necessary to consider Art. 6(1). *Id.* ¶ 973.

[247] Witness TF2-021 was nine years old when he was captured and eleven years old when he was sent on his first mission. *Id.* ¶ 968.

[248] *Id.* ¶¶ 967-72.

the Trial Chamber accepted other types of inconsistencies in witness testimony to convict the defendants of other crimes. In some cases, witnesses were unable to identify their ages,[249] months in which events occurred,[250] or dates on which events occurred.[251] Additionally, some witnesses could not tell time.[252] Witnesses struggled to estimate distances[253] and measurements,[254] as well as durations, numerical estimations,[255] and two-dimensional representations, such as maps.[256] Finally, some witnesses did not understand the adversarial court procedures of an international trial.[257]

The CDF Trial Chamber, like the AFRC Trial Chamber, was also concerned with communications challenges between judges, attorneys, and international witnesses who spoke many different languages.[258] In addition, the Trial Chamber considered witnesses' cultural and educational barriers.[259]

As in the AFRC Case, for the counts on which the CDF Trial Chamber decided to convict Fofana and Kondewa, the Trial Chamber considered testimonial deficiencies and inconsistencies, communications challenges, and cultural and educational barriers, but it determined the overall character of the testimony to be credible.

C. The Prosecutor v. Issa Hassan Sesay, Morris Kallon and Augustine Gbao

In *The Prosecutor v. Issa Hassan Sesay, Morris Kallon and Augustine Gbao* ("RUF Case"), the third relevant SCSL case involving evidentiary challenges in a child soldier case, two of the three defendants[260] from the Revolutionary United Front ("RUF") who were charged with, among other crimes, conscripting and enlisting child soldiers (Count 12),

---

[249] Trial Transcript at 22, CDF Case (Sept. 27, 2006). All CDF Case Transcripts can be accessed at *CDF Transcripts*, RESIDUAL SPECIAL COURT FOR SIERRA LEONE, http://www.rscsl.org/CDF_Transcripts.html (last visited Apr. 24, 2021).

[250] Trial Transcript at 54-55, CDF Case (June 21, 2004).

[251] Trial Transcript at 56-57, CDF Case (Sept. 13, 2004).

[252] Trial Transcript at 53-54, CDF Case (June 17, 2004).

[253] Trial Transcript at 29, CDF Case (Nov. 11, 2004); Trial Transcript at 104, CDF Case (Mar. 11, 2005); Trial Transcript at 69, CDF Case (Sept. 28, 2006); Trial Transcript at 88-89, CDF Case (Sept. 27, 2004).

[254] Trial Transcript at 104, 108, CDF Case (Sept. 23, 2004).

[255] Trial Transcript at 32, CDF Case (June 21, 2004); Trial Transcript at 22, CDF Case (Sept. 23, 2004).

[256] Trial Transcript at 38, CDF Case (Nov. 4, 2004).

[257] Trial Transcript at 45-46, 52, 68, CDF Case (May 22, 2006).

[258] Trial Transcript at 60-61, CDF Case (June 15, 2004); Trial Transcript at 16-17, CDF Case (June 18, 2004); Trial Transcript at 115-16, CDF Case (Sept. 27, 2004).

[259] A study of fifty-five prosecution witnesses indicated that eighteen (thirty-three percent) "were illiterate and/or had never attended any school" and seven (thirteen percent) "had attended school for only a few years." COMBS, *supra* note 13, at 65 (citing CDF Trial Transcripts).

[260] Defendant Gbao was found "not guilty" of conscripting and enlisting child soldiers but was found guilty of other crimes. RUF Case, *supra* note 191, at 686.

were found guilty, pursuant to Art. 6(1) of the Statute of the SCSL and punishable under Art. 4(c) of the Statute.[261] The RUF Trial Chamber focused on similar evidentiary considerations and concessions as those made by the AFRC and CDF Trial Chambers. The RUF Trial Chamber evaluated the evidence for witness credibility and general inconsistencies between multiple testimonies.[262] Specifically,

> [i]n assessing the credibility and reliability of oral witness testimony, the Chamber has considered factors such as the internal consistency of witness' testimony; its consistency with other evidence in the case; any personal interest witnesses may have that may influence their motivation to tell the truth; and observational criteria such as witnesses' demeanour, conduct and character. In addition, the Trial Chamber has considered the witnesses' knowledge of the facts on which they testify and the lapse of time between the events and the testimony.[263]

The Trial Chamber then conducted a credibility analysis of each witness. The Trial Chamber assessed four former child soldiers,[264] as well as three additional witnesses.[265]

The RUF Trial Chamber was concerned with many of the same discrepancies raised in prior SCSL cases, including ages,[266] dates,[267] durations,[268] and numerical estimations;[269] communications challenges;[270] and educational[271] and cultural barriers.[272] While the RUF Trial Chamber

---

[261] Prosecutor v. Sesay, SCSL-04-15-T, Sentencing Judgement (Apr. 8, 2009).

[262] The RUF Trial Chamber considered the following types of evidence: identification, RUF case, *supra* note 191, ¶¶ 492-94; hearsay, *id.* ¶¶ 495-96; accomplice, *id.* ¶¶ 497-98; circumstantial, *id.* ¶ 499; and expert evidence, *id.* ¶¶ 511-12. It considered whether testimony could be corroborated, *id.* ¶¶ 500-01, and it reviewed measures taken to protect witnesses, *id.* ¶¶ 504-05. Finally, it considered testimonial deficiencies regarding names and spellings of locations, *id.* ¶¶ 506-07; nicknames, *id.* ¶ 508; and time frames, *id.* ¶¶ 509-10.

[263] *Id.* ¶ 486 (citing Prosecutor v. Blagojevic, Case No. IT-02-60-T, Trial Chamber Judgement, ¶ 23 (Int'l Crim. Trib. for the Former Yugoslavia Jan. 17, 2005); Prosecutor v. Halilović, Case No. IT-01-48-T, Judgement, ¶ 17 (Int'l Crim. Trib. for the Former Yugoslavia Nov. 16, 2005).

[264] RUF Case, *supra* note 191, ¶¶ 579-94.

[265] *Id.* ¶¶ 595-603.

[266] Trial Transcript at 56, RUF Case (July 27, 2004).

[267] Trial Transcript at 74, RUF Case (July 19, 2004).

[268] Trial Transcript at 57, RUF Case (July 27, 2004).

[269] Trial Transcript at 50, 78, RUF Case (July 19, 2004); Trial Transcript at 35, RUF Case (July 15, 2004).

[270] Trial Transcript at 20-22, RUF Case (July 28, 2004).

[271] Out of 40 prosecution fact witnesses in the RUF Case, 19 (48 percent) "were illiterate and/or had never attended school" and three (eight percent) "had attended school for only a very short time." COMBS, *supra* note 13, at 65 (citing additional RUF Case Trial Transcripts).

[272] Trial Transcript at 70, RUF Case (Feb. 3, 2005) ("That which is not up to a month, we call it [a] week.").

considered these factors, as in the previous two SCSL cases, it found the testimony to be credible.

As these three SCSL cases illustrate, reliance on eyewitness testimony in general, and child witnesses in particular, presents significant evidentiary challenges and impediments to both fact-finding and presenting credible testimony at trial. The ICC[273] continues to grapple with evidentiary issues, because international criminal courts persist in relying heavily on eyewitness testimony, despite the fact that some scholars have raised concerns about this practice.[274]

IV. EVIDENTIARY CHALLENGES AND CRITIQUES OF *LUBANGA* EVIDENTIARY APPROACH

Lubanga presented significant challenges for the ICC evidentiary evaluation process. First, ICC investigators were forced to overcome major obstacles during testimony-gathering. Second, Trial Chambers struggled to verify testimony due to language, educational, and cultural barriers. Third, both courts and attorneys were beset by inconsistencies in testimony caused by investigative errors, translation issues, and contradictory witness statements.

Lubanga established critical evidentiary decision-making processes for the investigation and prosecution of the crimes of conscripting and enlisting child soldiers. Moreover, evidentiary issues demonstrated in *Lubanga* may apply to domestic cases regarding potentially unreliable eyewitness testimony. Therefore, the ICC must recognize the burdens created by evidentiary barriers and the harm they can cause to both witnesses and fact-finding procedures.

A. Evaluating Evidentiary Issues Outside the Case Law Context

i. Gathering Testimony is Difficult Due to Safety Concerns and Logistical Barriers

As the multi-year ICC investigation in *Lubanga* highlighted, one significant challenge that ICC investigators faced in the early stages of an international criminal case was gathering reliable testimony in the field. The ICC confronted three major obstacles during testimony-gathering. First, investigators faced security challenges that made it difficult to obtain information and to connect with witnesses.[275] Specifically, the areas in which

[273] Domestic courts also struggle to handle testimony from child witnesses (or witnesses who were children at the time of the crime). *See, e.g.*, Lacy & Stark, *supra* note 14.

[274] Combs, *supra* note 16, at 56 ("[W]itness testimony usually forms the exclusive basis for international criminal convictions, and that in itself is a problem.").

[275] *See* Trial Chamber Judgment, *supra* note 1, ¶¶ 151-68.

the most heinous crimes were committed were also the ones that were too dangerous to investigate,[276] because the forces controlling these regions were often hostile to the investigators.[277] Second, logistical difficulties, like impassible or nonexistent roads, made travel challenging.[278] Third, investigators faced language and cultural barriers,[279] similar to the barriers later faced at trial, once they connected with witnesses.[280]

ii. Language and Educational Barriers Impede the Chamber's Ability to Verify Testimony

Once testimony has been gathered, it must also be verified. Within the context of international criminal law, while:

> [t]here was once reason to believe that the incidence of [testimonial] deficiencies would decline over time, and the fact that they did not provides clues as to their causes. What did decline, however, was the Trial Chambers' willingness to credit prosecution witnesses and rely on their testimony. Indeed . . . over time [international criminal law has] strengthened its commitment to factual accuracy and, more broadly, to the beyond-a-reasonable-doubt standard for convictions.[281]

An initial challenge in assessing potential testimonial deficiencies is verifying basic information. Trial Chambers rely on witness candor in the absence of accurate identification.[282] As the AFRC, CDF, and RUF Cases from the SCSL highlight, there are many barriers to confirming information—and to eliciting accurate testimony at trial. For example, Trial Chambers struggle to communicate with international witnesses due to

[276] *See* COMBS, *supra* note 13, at 147.

[277] *See* Trial Chamber Judgment, *supra* note 1, ¶¶ 151-68.

[278] *See* COMBS, *supra* note 13, at 147.

[279] *See* Trial Chamber Judgment, *supra* note 1, ¶¶ 151-68.

[280] For example, one study by John Jackson and Yassin Brunger found that witness statements frequently included inaccuracies because "investigators did not understand the information they were being provided." Combs, *supra* note 16, at 112. Furthermore, the investigators "failed to be culturally sensitive" and asked "inappropriate questions." John D. Jackson & Yassin M. Brunger, *Fragmentation and Harmonization in the Development of Evidentiary Practices in International Criminal Tribunals*, *in* PLURALISM IN INTERNATIONAL CRIMINAL LAW 159, 173-74 (Elies van Sliedregt & Sergey Vasiliev eds., 2014). Furthermore, the investigators "failed to be culturally sensitive" and asked, "inappropriate questions." *Id.*

[281] Combs, *supra* note 16, at 109 (Combs' conclusions are based on data and regression analysis of International Criminal Tribunal for Rwanda cases.).

[282] *See id.* at 58 (This was specifically noted in *Lubanga*: the Trial Chamber relied on witness testimony about anatomical indicators of age.); *see also* COMBS, *supra* note 13, at 145 (Furthermore, "[l]ack of documentation stymies efforts to ascertain . . . basic facts.").

translation and interpretation errors,[283] as well as educational[284] and cultural barriers that make witnesses either incapable of conveying the necessary information or generally unwilling to testify fully.[285] In addition, international courts do not necessarily consider cultural differences when assessing witness testimony.[286] For example, certain cultures view the concept of "childhood" differently from the way Western cultures do.[287] This makes it difficult to elucidate accurate age information from witnesses.

A significant passage of time between the crime and the trial also presents a substantial challenge to maintaining an accurate memory of the events. Memory naturally fades over time.[288] Furthermore, if significant time has passed, even a well-intentioned witness might hear additional information about a case that affects his or her perception of the events.[289] This information could come from interview questions (witnesses may be interviewed multiple times), the national or international news, or discussions with friends and family.[290] In fact, one study of International Criminal Tribunal for Rwanda cases concluded that "the number of statements/testimonies that a witness provided was a very strong predictor of serious inconsistencies."[291] Furthermore, witnesses or victims of violent crimes are more likely than witnesses of non-violent events to misperceive events because of the effect of stress on perception.[292]

---

[283] *See* Joshua Karton, *Lost in Translation: International Criminal Tribunals and the Legal Implications of Interpreted Testimony*, 41 VAND. J. TRANSNAT'L L. 1, 40-41 (2008); *see also* COMBS, *supra* note 13, at 66-70.

[284] *See* COMBS, *supra* note 13, at 63-66.

[285] *See id.* at 79-81.

[286] Teresa A. Doherty, *Evidence in International Criminal Tribunals: Contrast Between Domestic and International Trials*, 26 LEIDEN J. INT'L. L. 937, 938 (2013).

[287] TIM KELSALL, CULTURE UNDER CROSS-EXAMINATION: INTERNATIONAL JUSTICE AND THE SPECIAL COURT FOR SIERRA LEONE 151 (2009) (analyzing the CDF Case at the SCSL). Specifically, "[r]elationships . . . which would doubtless be regarded as neglectful or abusive in many societies, are legitimised in southern Sierra Leone by a local ideology anchored on the belief that there is 'no success without struggle.'" *Id.* at 152.

[288] *See* Hadyn D. Ellis, *Practical Aspects of Face Memory*, *in* EYEWITNESS TESTIMONY: PSYCHOLOGICAL PERSPECTIVES 12, 23-25 (Gary L. Wells & Elizabeth F. Loftus eds., 1984).

[289] *See* David F. Hall et al., *Postevent Information and Changes in Recollection for a Natural Event*, *in* EYEWITNESS TESTIMONY: PSYCHOLOGICAL PERSPECTIVES 124 (Gary L. Wells & Elizabeth F. Loftus eds., 1984).

[290] *See* COMBS, *supra* note 13, at 17. Combs examined six International Criminal Tribunal for Rwanda cases and three SCSL cases and "found that, on average, approximately 50 percent of witnesses in those cases testified seriously inconsistently with their previous statements/testimonies." *See* Combs, *supra* note 16, at 107; COMBS, *supra* note 13, at 118-22.

[291] Combs, *supra* note 16, at 108.

[292] *See* Douglas P. Peters, *Eyewitness Memory and Arousal in a Natural Setting*, *in* 1 PRACTICAL ASPECTS OF MEMORY: CURRENT RESEARCH AND ISSUES: MEMORY IN EVERYDAY LIFE 89, 94 (Michael M. Gruneberg et al. eds., 1988).

iii. Inconsistencies in Testimony May Result in Important Testimony Being Excluded

Many of the factors used to evaluate testimonial deficiencies are also applicable when evaluating testimonial inconsistencies (i.e. contradictory statements).[293] For example, an illiterate witness cannot review each transcribed statement taken throughout the case to verify its accuracy.[294] In addition, using multiple translators throughout the case may produce discrepancies, especially if some of the translators are connected to the case and harbor ulterior motives.[295] Also, investigative errors, either unintentional or intentional,[296] may lead to inconsistencies.[297] However, extremely consistent statements should also be treated with caution because "it is possible that perjuring witnesses—and particularly perjuring witnesses who are lying in order to receive tangible and substantial benefits—take greater care than truthful witnesses to keep their representations consistent."[298]

In evaluating testimonial inconsistencies when witnesses make multiple statements, Trial Chambers concede that some inconsistencies are serious, whereas others can be reconciled by the factors previously discussed. Specifically, "an inconsistency or omission [may] be serious either if it pertained to a key issue in the trial or if it pertained to the kind of fact that one is unlikely to forget."[299] However, during lengthy testimony, Trial Chambers may decide to admit certain portions of the testimony while excluding others.

iv. Evidentiary Issues in Domestic Criminal Cases Parallel Those Issues in *Lubanga*

Many of the evidentiary challenges that ICC prosecutors faced in *Lubanga* also persist in domestic criminal cases, despite the fact that prosecutors in the United States may face fewer linguistic and cultural barriers. Eyewitness testimony in domestic cases is similarly prevalent and

[293] *See* COMBS, *supra* note 13, at 122.

[294] *Id.*

[295] *Id.* at 124.

[296] Intentional investigative "errors" are less common than witnesses allege, but they do sometimes occur. *See* Combs, *supra* note 16, at 113-14.

[297] *See* COMBS, *supra* note 13, at 126. ("Interviews . . . generate off-the-record stories of investigators who at best lack an adequate understanding of the conflict that they are investigating and the culture and habits of the people who are to be witnesses, and who at worst are lazy and/or incompetent.").

[298] Combs, *supra* note 16, at 111.

[299] COMBS, *supra* note 13, at 121; *see* Combs, *supra* note 16, at 67 (defining a "serious" inconsistency: for example, "when a witness failed to mention in his previous statements/testimonies a fact that was central to his testimony").

may be unreliable,[300] potentially leading to wrongful convictions[301] in some instances.[302] Similar to witnesses in ICC cases, domestic witnesses' memories fade over time.[303] Furthermore, witnesses, including victims of violent crimes, are more likely than witnesses of nonviolent acts to misperceive events[304] due to the effects of fear and psychological stress on perception.[305] These inaccuracies include incorrectly identifying the numbers[306] and identities[307] of the perpetrators. In addition, a witness's memory may be altered if he or she learns additional information about an event[308] through the news, casual conversations, or facts gleaned during several rounds of pretrial and trial questioning.[309] These challenges mirror the evidentiary issues plaguing ICC prosecutors. Similar to ICC judges, a United States judge's ability to discern truth and falsity when evaluating a witness may be crucial to threshold admissibility determinations.

B. Critiques of the ICC's Evidentiary Process in Lubanga

The crime of conscripting and enlisting child soldiers under Art. 8(2)(e)(vii) of the Rome Statute was an issue of first impression for the ICC

---

[300] Recent DNA testing indicates that nearly 80 percent of wrongful convictions in U.S. criminal cases involved errors in eyewitness testimony. *See* Brandon L. Garrett, *Judging Innocence*, 108 COLUM. L. REV. 55, 78-79 (2008).

[301] *See* BRIAN L. CUTLER & STEVEN D. PENROD, MISTAKEN IDENTIFICATION: THE EYEWITNESS, PSYCHOLOGY, AND THE LAW 8-13 (1995); Douglas J. Narby et al., *The Effects of Witness, Target, and Situational Factors on Eyewitness Identifications, in* PSYCHOLOGICAL ISSUES IN EYEWITNESS IDENTIFICATION 23, 24-28 (Siegfried L. Sporer et al. eds., 1996); Brian L. Cutler et al., *Conceptual, Practical, and Empirical Issues Associated with Eyewitness Identification Test Media*, *in* ADULT EYEWITNESS TESTIMONY: CURRENT TRENDS AND DEVELOPMENTS 163, 166-81 (David F. Ross et al. eds., 1994).

[302] The author is not making a value judgment about eyewitness testimony in domestic cases. Rather, the author has provided domestic research as a point of comparison.

[303] *See* JOHN W. SHEPHERD ET AL., IDENTIFICATION EVIDENCE: A PSYCHOLOGICAL EVALUATION 80-86 (1982) (describing a study in which subjects' memories declined significantly over an eleven-month period).

[304] *See* ELIZABETH LOFTUS ET AL., EYEWITNESS TESTIMONY: CIVIL AND CRIMINAL 25 (LexisNexis) (6th ed. 2007).

[305] *See* Charles A. Morgan III et al., *Accuracy of Eyewitness Memory for Persons Encountered During Exposure to Highly Intense Stress*, 27 INT'L J. L. & PSYCHIATRY 265, 268, 272 (2004) (studying the effects of high- and low-stress situations on military service members).

[306] *See* Brian R. Clifford & Clive R. Hollin, *Effects of Type of Incident and the Number of Perpetrators on Eyewitness Memory*, 66 J. APPLIED PSYCH. 364, 369 (1981).

[307] *See* John C. Brigham et al., *The Effect of Arousal on Facial Recognition*, 4 BASIC APPLIED SOC. PSYCH. 279, 291 (1983); Sven-Åke Christianson & Elizabeth F. Loftus, *Memory for Traumatic Events*, 1 APPLIED COGNITIVE PSYCH. 225, 227 (1987); Saul M. Kassin, *Eyewitness Identification: Victims Versus Bystanders*, 14 J. APPLIED SOC. PSYCH. 519, 519-20 (1984).

[308] There are many opportunities for new information to alter a witness's recollection over the course of a lengthy case. *See* COMBS, *supra* note 13, at 14-15.

[309] *See* Hall, *supra* note 289, at 124.

in *Lubanga* and was therefore a critical precedent-setting decision.[310] The Trial Chamber in *Lubanga* relied heavily on three SCSL cases: it applied the factors developed in the AFRC, CDF, and RUF Cases to evaluate *Lubanga* witnesses' and intermediaries' potential testimonial deficiencies and inconsistencies.[311]

The staggering amount of evidence presented in this case—more than 1300 pieces of physical evidence, as well as testimony from more than 65 witnesses[312]—overwhelmingly indicates that Lubanga committed the crimes of conscripting and enlisting children under the age of 15 and using them to participate actively in hostilities under Art. 8(2)(e)(vii) of the Statute, and that Lubanga was individually criminally responsible as a co-perpetrator under Art. 25(a)(3) of the Statute. While the case was ultimately correctly decided, some of the Trial Chamber's determinations about witness credibility and reliability were troublesome, and they led to the unfair exclusion of some potentially valuable witnesses and intermediaries.

As Judge Benito suggested in her dissenting opinion, many of the excluded victim-witnesses should have been permitted to participate in the trial as victims.[313] The Trial Chamber's decision to exclude victims from the proceedings was misguided for several reasons. First, trials are extreme emotionally taxing, especially on children. Individuals would not voluntarily subject themselves to this trauma unless they had true and compelling stories to tell. Second, witnesses put themselves and their families at significant risk by testifying.[314] The security precautions taken by the Prosecution are not necessarily protective enough, especially once witnesses return home, since the FPLC retains a powerful presence in the DRC.[315] Furthermore, these protections do not continue after the completion of the trial.[316] In the meantime, witnesses' families in the DRC are vulnerable to retribution.[317] In addition, witnesses invest significant time to prepare for interviews and to provide multiple pretrial and trial statements. Finally, witnesses may face financial hardships related to travel, lodging, and meals that the ICC cannot guarantee will be fully covered.[318] Agreeing to testify at an international criminal trial is not a decision that a witness would take lightly, and individuals would not assume these risks and hardships only to testify either inaccurately or deliberately falsely.

---

[310] The issue of child soldiers is one that the ICC has only tackled a few times since *Lubanga*. *See, e.g.*, Prosecutor v. Ntaganda, ICC-01/04-02/06-2359, Judgment (July 8, 2019); Prosecutor v. Ongwen, ICC-02/04-01/15-1762, Trial Judgment (Feb. 4, 2021).

[311] *See supra* Section III for a thorough description of these factors.

[312] *See* Trial Chamber Judgment, *supra* note 1, ¶ 11.

[313] *See* Separate and Dissenting Opinion of Judge Benito, *supra* note 182.

[314] *See* Trial Chamber Judgment, *supra* note 1, ¶¶ 151-68.

[315] *See id.*

[316] *See id.*

[317] *See id.*

[318] *See id.* ¶¶ 198-202.

The Trial Chamber's decision to exclude several intermediaries—as well as some of the witnesses with whom they worked, who were excluded because the Trial Chamber was concerned that the intermediaries had coached them to lie[319]—was also concerning. The suggestion that intermediaries lied, or coached witnesses to lie,[320] was unpersuasive. On the one hand, because the intermediaries put themselves in danger while working in the DRC,[321] they might have sought to make the risks worthwhile. However, intermediaries are told very little about the cases on which they work,[322] partially to minimize the likelihood that biases or ulterior motives will affect their work. Therefore, besides coaching witnesses to lie about their ages (which was not the only factor that the Trial Chamber considered in making these determinations), it would be difficult to concoct substantive lies that would significantly damage the credibility of the totality of their testimony. Furthermore, because intermediaries are not paid[323] and are serving the ICC honorably, they might be less likely to act dishonestly.

The Trial Chamber conceded at the outset of the *Lubanga* trial that it would consider factors including, but not limited to, the length of time between the crimes and the trial, trauma that caused somewhat conflicting recollections, and communication barriers, among other considerations. However, some witnesses and intermediaries were excluded based on what appeared to be minor deficiencies or inconsistencies in their testimonies. Fortunately, even after excluding several witnesses and intermediaries, the Trial Chamber heard admissible testimony from more than enough Prosecution, Defense, and expert witnesses to convict Lubanga of horrific crimes against children.[324]

The evidentiary challenges faced by ICC prosecutors persist in domestic cases as well. Judges, attorneys, and witnesses in U.S. criminal cases may face fewer language and cultural barriers (although these do exist). However, eyewitness testimony in domestic cases, while commonly used, is subject to the same deficiencies discussed in this Article in the context of ICC cases. While many legal scholars, law enforcement professionals, and attorneys concede that memory fades and can be reshaped over time, and that trauma affects a witness's perception of the crime, judges and juries continue to find eyewitness testimony compelling. While evidentiary issues are heightened in the international context, they are by no means unique to the ICC.

While this Article did not analyze sentencing issues, it is also concerning that Lubanga only received a 14-year sentence for his heinous

---

[319] *See id.* ¶¶ 37-41.
[320] *See* Trial Chamber Judgment, *supra* note 1, ¶ 180.
[321] *See id.* ¶¶ 151-61.
[322] *Id.* ¶ 183.
[323] *Id.* ¶ 198.
[324] *See id.* ¶ 11.

crimes.[325] In fact, Lubanga's sentence was reduced by six years because he was imprisoned during the investigation and trial.[326] Lubanga was ordered to pay significant reparations to the Victim Compensation Fund.[327] However, because Lubanga allegedly could not afford to pay reparations, the DRC government was asked to assist with the payments.[328] Because the FPLC remains a significant presence in the DRC, Lubanga's victims may never receive reparations. Perhaps some of the excluded witnesses could have provided sufficiently compelling testimony to influence the Chamber during sentencing to extend Lubanga's term of imprisonment.

While some of the Trial Chamber's evidentiary determinations raised significant concerns, ultimately, the Trial Chamber's most important conclusion was that Lubanga was guilty of conscripting and enlisting child soldiers under Arts. 8(2)(e)(vii) and 25(3)(a) of the Statute.

V. CONCLUSION

ICC prosecutors in *Lubanga* tackled many evidentiary hurdles that continue to beleaguer the ICC to this day. As cases such as *Lubanga* proceed from security concerns, as well as language and cultural barriers, during the investigatory process; to miscommunication and errors during pretrial interviews; to determining witness credibility; to evaluating testimonial deficiencies and inconsistencies, it is clear that the road to an international criminal conviction is beset with challenges.

Since *Lubanga* was decided, several additional child soldier cases have been tried before the ICC.[329] However, potential war criminals—both within and outside the DRC—continue to conscript and enlist child soldiers, often with apparent impunity. The challenges discussed in this Article persist into the third decade of the ICC's existence. As the ICC strives to prosecute additional child soldier cases in the future, the concerns explored in this Article suggest that procedural reforms are necessary. Reforms[330] might include hiring more experienced translators, increasing the number of investigators, and punishing witnesses who intentionally perjure themselves. The ICC might also consider a larger annual investment of resources into its investigations and prosecutions, as well as a more aggressive and dogged

---

[325] *See generally* Lubanga Decision on Sentence, *supra* note 9.

[326] *Id.* ¶ 108.

[327] *See generally* Lubanga Decision Setting Reparations, *supra* note 169.

[328] *See generally id.*

[329] *See, e.g.*, Prosecutor v. Ntaganda, ICC-01/04-02/06-2359, Judgment (July 8, 2019); Prosecutor v. Ongwen, ICC-02/04-01/15-1762, Trial Judgment (Feb. 4, 2021).

[330] On a larger scale, one scholar suggested that the ICC should consider the more controversial move of transitioning toward a non-adversarial process of elucidating testimony. *See* COMBS, *supra* note 13, at 302-04 ("Whereas, in an adversarial system, testimony is elicited through a formal interrogation, in a non-adversarial trial, witnesses convey their testimony through exchanges that bear greater resemblance to a[n] informal conversation than a judicial interrogation.").

approach to its cases. Regardless of whether the ICC ultimately decides to make structural changes, each judge's ability to make both accurate determinations about witness credibility and effective rulings about admissible testimony will be critical to obtaining successful criminal convictions and to achieving justice for victims.

THE FUTURE OF KOREAN REGULATION ON INITIAL COIN OFFERINGS

Whayoon Song[*]

I. INTRODUCTION

Market regulators are in limbo given the lack of consensus over how to best regulate cryptocurrencies.[1] There is particular uncertainty regarding initial coin offerings, or ICOs.[2] In the crypto ecosystem, an ICO is the process of raising funds to proceed a project in exchange for tokens (also referred to as coins—a type of cryptocurrency).[3] International regulation of ICOs differs by country. Some regulators exempt ICO firms from regulation in order to promote the blockchain industry. Whereas other governments implement stronger regulations to protect investors from fraud involving cryptocurrency. Because views regarding cryptocurrency vary by country, vastly different methods and degrees of international regulations exist. For example, the United States attempts to protect investors by proactively regulating ICOs as investment contracts subject to securities regulations.[4] By contrast, some countries, such as China, have banned all cryptocurrency transactions and

* Ph.D. in Law, Korea Exchange. E-mail: whayoon@krx.co.kr. This paper is developed and modified from the author's LL.M research paper supervised by Professor Rodrigus of the University of Georgia Law School from 2018-2019. The author appreciates the delicate advice and support from Professor Rodrigus of University of Georgia Law School and Lenardo Mazor, Esq. All errors are the author's own. This paper is the author's personal opinion and not the official opinion of Korea Exchange. The author takes sole responsibility for the accuracy of all citations to Korean-language sources throughout this article.

[1] The term cryptocurrency "refers to an asset that is issued and transferred using distributed ledger or blockchain technology, including, but not limited to, so-called 'virtual currencies,' 'coins,' and 'tokens.' SEC, *Framework For "Investment Contract" Analysis of Digital Assets* (April 3, 2019), https://www.sec.gov/ICO; Cryptocurrency is defined as "decentralized, peer-to-peer digital currency that is used similarly to money." Julianna Debler, *Foreign Initial Coin Offering Issuers Beware: The Securities and Exchange Commission is Watching*, 51 CORNELL INT'L L.J. 245, 249 (2018).

[2] The term initial coin offering ("ICO") is derived from the traditional Initial Public Offering in securities markets. The aim of both IPO and ICO is to raise funds but there are many differences. For examples, shares in IPOs are sold through exchanges regulated by financial regulators, so investor protection is well established. When it comes to ICOs, on the other hand, issuers sell tokens directly to the public at the beginning stage of development. Stephen J. Choi & A.C. Prichard, *Securities Regulation,* 396-405 (4th ed. 2015); Marco Dell Eraba, *Initial Coin Offering: The Response of Regulatory Authorities*, 14 N.Y.U. J.L. & BUS. 1107, 1110-14 (2018).

[3] Dell Eraba, *supra* note 2 at 1110; Maria Fonsea, *ICOs and Blockchain Token Funding,* INTELLIGENT HQ (May 5, 2017), http://www.intelligenthq.com/finance/icos-and-blockchain-token-funding (last visited July 4, 2020); SEC, *supra* note 1.

[4] Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934: the DAO, Exchange Act Release No. 81207, 117 SEC Docket 5 (July 25, 2017).

ICOs.[5] Other countries, such as Singapore, have attempted to formulate clear regulations to promote ICOs.[6]

The situation in South Korea is also chaotic. Leading up to 2017, many Korean investors were forced to buy Bitcoin and pay more money on the Korean market, so called 'Kimchi premium.'[7] Being concerned about excessive volatility and fraud related to cryptocurrency, the Korean government implemented such drastic measures as banning ICOs.[8] With these regulatory changes, the market quickly plummeted. The Korean government has been deliberating the side effects of regulation and has taken a cautious stance in adopting new regulations. Additionally, the lack of proper regulations has made the situation worse because cryptocurrency industries, including ICO firms, do not clearly know what is illegal, and firms that want to implement ICOs seem to go outside of Korea to other countries that allow ICOs, such as Singapore. Given these situations, it is important to examine how to properly regulate cryptocurrencies.

This paper argues that the South Korean government needs to take advantage of the existing regulations, while also focusing on how to regulate security tokens and utility tokens.[9] Since regulators started to strictly regulate cryptocurrencies, many countries applied securities regulations to tokens, but numerous issues remain regarding how to best regulate tokens with security features.[10]

Considering the South Korean government's stance that new regulations should follow the global trend,[11] this paper draws conclusions by

---

[5] Dirk Zetsche, Ross P. Buckley, Douglas W. Armer & Linus Fohr, *The ICO Gold Rush: It's a Scam, It's a Bubble, It's a Super Challenge for Regulators,* 31 (European Banking Institute Working Paper Series No 18, 2018).https://papers.ssrn.com/sol3/papers.cfm?abstract_id=3072298.

[6] Press Release, Monetary Authority of Singapore (MAS), MAS Clarifies Regulatory Position on the Offer of Tokens in Singapore (Aug. 1, 2017).

[7] BBC, *Bitcoin: South Korea Sways Cryptocurrency Prices – but How?*, (Jan. 17, 2018), https://www.bbc.com/news/business-42713314; Koreans paid much more to buy bitcoin in 2017 than Americans. Kyoung Jin Choi, Alfred Lehar & Ryan Stauffer, *Bitcoin Microstructure and the Kimchi Premium,* (Jan. 10, 2020), https://ssrn.com/abstract=3189051.

[8] Financial Services Commission, *Cryptocurrency Task Force Meeting to Review the Actions of the Relevant Institutions* (Sept. 4, 2017), https://www.fsc.go.kr/no010101/72809.

[9] Many times, the term 'token' and 'coin' is used interchangeably. However, coins are the digital currency for payment purpose with Bitcoin as a prominent example. Tokens, on the other hand, represent assets which give holders the right to participate in the network. *What is the Difference between Coins and Tokens*, BONPAY (Mar. 13, 2018), https://medium.com/@bonpay/what-is-the-difference-between-coins-and-tokens-6cedff311c31.

[10] The authorities in three of the countries featured in this paper—the U.S., Singapore, and Japan—make clear that tokens with securities features are regulated as securities. *See* Part III *infra*.

[11] On November 13, 2018, the government official said that the Korean government would measuredly adopt the regulations while keeping an eye on the global trend. FSC, *Held the 1st Meeting of Digital Currency Institutionalization*, (Nov. 17, 2016) https://www.fsc.go.kr/no010101/72440?srchCtgry=&curPage=2&srchKey=sj&srchText=&srchBeginDt=2016-11-01&srchEndDt=2016-11-30.

comparing global regulations with Korean regulations. This paper compares the U.S., Singapore, and Japan because of the level of regulation on ICO and concentration of ICOs in each country. In the U.S., regulators have clearly applied securities regulation to cryptocurrencies with features akin to securities. In Singapore, regulators applied securities regulations for ICOs. Finally, in Japan, regulators recently introduced new ICO regulations.

This Article proposes that the Korean government should implement the regulatory mechanism in the Financial Investment Services and Capital Market Act (South Korean Securities Regulation Act, FSCMA).[12] Although IPOs and ICOs are different, the same needs for investor protections, fairness, transparency, and efficiency of the market apply. Moreover, ICOs provide fundraising sources for ICO firms, which must be balanced with the need to protect investors. Finally, such an approach would align with global regulation because most countries use or are considering using securities regulation in ICO regulation. In principle, this paper proposes that ICO firms must comply with the FSMCA. However, considering the regulatory burden for ICO firms and the vulnerability of the general public, the regulator can allow ICO firms to use exemptions such as crowdfunding mechanisms. It should limit market participants to professional investors and allow brokerage firms to screen financial conditions of investors, ICO firms, and the project progress of ICO firms. Regulators should require registration and disclosure to prevent information asymmetry between investors and ICOs firms.

This research will proceed as follows. Part II will introduce the features of cryptocurrency and distributed ledgers. Part III will investigate the current regulation and ICO situation in Korea. Next, Part IV will examine the global response for ICOs regulation–specifically in the U.S., Singapore, and Japan. Subsequently, Part V will propose the regulation mechanism Korea should adopt. Finally, Part VI concludes that for ICO regulation, the existing FSCMA should be used to protect investors and eventually support the development of the blockchain industry.

II. INTRODUCTION TO CRYPTOCURRENCY AND DISTRIBUTED LEDGERS

Cryptocurrency regulations remain unclear and vary between countries.[13] Some countries use 'currency' to describe cryptocurrency's payment function and other countries use 'asset' to emphasize its asset features such as crypto asset (Japan) and virtual asset (South Korea, FATF).

[12] Securities-Related Class Action Act, Act No. 8635, August 3, 2007, *amended by* Act No. 11845, May 28, 2013 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/kor_service/lawView.do?hseq=29730&lang=ENG.

[13] Library of Congress, *Regulation of Cryptocurrency Around the World*, https://www.loc.gov/law/help/cryptocurrency/world-survey.php

Some countries use 'crypto' to describe its features made from encryption technology and others use 'digital' to express its digital value.[14]

Cryptocurrency started appearing right after the financial crisis in 2008 to address the problems of a centralized financial system. In September 2008, right after the financial institutions went bankrupt, the pseudonymous Satoshi Nakamoto published the white paper on Bitcoin, the first cryptocurrency, which lamented that entire financial systems reliance on centralized authority.

This Bitcoin white paper proposed a revolutionary system of exchange using blockchain technology in which all transactions are recorded in a distributed and decentralized ledger instead of going through centralized systems managed by third parties, such as banks.[15] Satoshi intended to prevent double-spending problems through this pure peer-to-peer network in which transactions are time-stamped by hashing and are distributed in the network.[16] As transaction records are accumulated as blocks, which are accumulations of transaction data, each block is interlinked, establishing the chain. In this distributed ledger system, proof-of-works ensure the reliability of the distributed ledger. Transaction records are verified by participants and without proof-of-work, transaction records cannot be reversed.[17] This system enhances transparency and provides peer-to-peer accountability, which was for want after the 2008 financial crisis.

Some cryptocurrencies are referred to as coins which operate independently on their own platform, such as Bitcoin. Some cryptocurrencies are referred to as tokens which operate on the other existing coin platform.[18] These terms are used interchangeably.[19]

Essentially, there are two types of tokens – a non-security type and a security type. Security type tokens are tokens with securities features and non-security tokens are tokens without such features. Securities features include the right to participate the management of projects such as voting rights and dividends, which will become the asset of investors. Consequently, the Financial Market Supervisory Authority of Switzerland, names security

---

[14] Youngeun Cho, Strengthening Protection Regulation of Crypto-Asset Users in Japan, NATIONAL ASSEMBLY RESEARCH SERVICE, Vol. 38, 3 (Apr. 19, 2019), https://www.assembly.go.kr/assm/notification/news/news01/bodo/bodoView.do?bbs_id=ANCPUBINFO_05&bbs_num=48744&no=6797&CateGbn=&Gbntitle=$paramMap.Gbntitle.

[15] TIMOTHY G. MASSA, IT'S TIME TO STRENGTHEN THE REGULATION OF CRYPTO-ASSETS, ECONOMIC STUDIES AT BROOKINGS 9, (Mar. 2019), https://www.brookings.edu/wp-content/uploads/2019/03/Timothy-Massad-Its-Time-to-Strengthen-the-Regulation-of-Crypto-Assets-2.pdf; Satoshi Nakamoto, *Bitcoin: A Peer-to-Peer Electronic Cash System*, BITCOIN.COM, http://bitcoin.org/bitcoin.pdf.

[16] Nakamoto, *supra* note 15.

[17] *Id*.

[18] Ke Wu, Spencer Wheatley and Didier Sornette, *Classification of Cryptocurrency Coins and Tokens by the Dynamics of Their Market Capitalizations*, THE ROYAL SOCIETY PUBLISHING 2, (Sept. 5, 2018) https://royalsocietypublishing.org/doi/10.1098/rsos.180381.

[19] *Difference between Coins and Tokens*, *supra* note 9.

tokens as Asset tokens in the FINMA's Guideline in 2017.[20] Tokens without security features are non-security tokens. This non-security type will be categorized into payment tokens and utility tokens.[21] Payment tokens are used as a means of exchange for values as Bitcoin is exchanged for items in the real world.[22] Utility tokens are access rights to the specific distributed ledger platform and used to barter for some service.[23] These three concepts – security tokens, payment tokens and utility tokens – are not mutually exclusive. Most tokens are designed and used as utility tokens but even though they are initially designed as utility tokens, they will be regarded as security given that they have security features for regulatory purpose.[24] In short, cryptocurrencies have revolutionized transactions replacing centralized governance with blockchain technology.

III. CURRENT KOREAN REGULATION AND PROBLEMS

The South Korean government has taken a very conservative and careful approach toward regulating ICO. Other than the ICO ban, not many regulations have yet been introduced. This section will describe the current regulation of ICOs in South Korea, and the problems associated with the present approach.

A. Current Korean Regulation

In 2017, South Korea fell in love with cryptocurrency. The price of Bitcoin on the Korean market was higher than in other markets, a situation referred to as the "Kimchi Premium."[25] However, so far, there have been few clear regulations regarding ICOs other than the ICO ban. To respond to the speculative market situation and demands to create the proper regulation, the

[20] FINMA, *Guidelines for Enquiries Regarding the Regulatory Framework for Initial Coin Offerings (ICOs*) (Feb. 16, 2018) https://www.finma.ch/en/news/2018/02/20180216-mm-ico-wegleitung/. FINMA classifies tokens into payment tokens, asset tokens, utility tokens according to their functions.

[21] Apolline Blandin et al., *Global CryptoAsset Regulatory Landscape Study*, 18, CAMBRIDGE CENTRE FOR ALTERNATIVE FINANCE (Jan. 1, 2019) https://www.jbs.cam.ac.uk/wp-content/uploads/2020/08/2019-04-ccaf-global-cryptoasset-regulatory-landscape-study.pdf. This classification is similar to those detailed in the guideline of FINMA, the Swiss financial regulator. For regulatory purposes, FINMA's guideline divides cryptocurrency into payment tokens, utility tokens, and asset tokens (which are similar to security token). If the sale takes place before tokens are issued or exchanged (i.e., pre-financing, pre-sale), the tokens are regarded as securities, meaning the securities regulation will apply. Anti-Money laundering law apply only to payment tokens. FINMA, *supra* note 20.

[22] Blandin et al., *supra* note 21.

[23] *Id.*

[24] If utility tokens are used for payment, then they will be regulated as payment tokens. FINMA's guideline anti-money laundering (AML) laws will apply only to Payment Tokens.

[25] Jin Choi et al., *supra* note 7.

South Korean government organized the Cryptocurrency Task Force.[26] This task force was led by the Financial Supervisory Committee ("FSC"), which is the governmental agency that regulates financial markets in South Korea. In September 2017, the Cryptocurrency Task Force announced in a press release that it would introduce several strong regulations intended to calm speculation in the cryptocurrency market and protect investors.[27] Furthermore, worrying about the speculative situation, the South Korean government banned all types of ICOs that same month.[28]

There have been few clear legislative actions since the September 2017 press release announcements. However, just as the Cryptocurrency Task Force emphasized, existing FSCMA will apply, especially for anyone who conducts securities type ICOs.[29] There is no specific government guidance for distinguishing between securities type ICOs and non-securities type ICOs. The government has persistently taken the prudent approach to creating new ICO regulation, worrying that it may give the wrong signal to markets and the industry as showing the government's approval of ICOs.[30]

In September 2017, the government also announced it would recommend that the cryptocurrency dealers' association develop rules and guidelines providing for self-regulating the cryptocurrency market, emphasizing investor protection.[31] In accordance with this announcement, exchanges and blockchain companies established the South Korean Blockchain Association ("KBCA") and confirmed a self-regulatory framework in April 2018.[32] This framework benchmarked many features of securities regulation to protect investors and guarantee transparency and stability.[33]

The framework also established a guideline that strengthened the process and transparency of listing coins. Under this guideline, exchanges will use the listing guideline provided by the KBCA.[34] The KBCA will provide the information evaluating new coins to exchanges in order for

---

[26] *Cryptocurrency Task Force Meeting to Review the Actions of the Relevant Institutions*, *supra* note 8.

[27] *Id*.

[28] *Id.*

[29] *Id.*; Jung Min Lee, Joon Young Kim & Samuel Yim, *The Financial Technology Law Review (3rd Edition)*, LAW BUSINESS RESEARCH LTD., at 252 (May 29, 2020), https://www.kimchang.com/en/insights/detail.kc?sch_section=5&idx=21434.

[30] Lee et al., *supra* note 29; Financial Services Commission, *ICO Survey Results and Future Countermeasures*, at 4 (Jan. 31, 2019), https://www.fsc.go.kr/no010101/73527.

[31] *Cryptocurrency Task Force Meeting to Review the Actions of the Relevant Institutions*, *supra* note 8.

[32] Korea Block Chain Association*, Cryptocurrency Exchange Self-Regulation Briefing Session*, (Dec. 15, 2017) https://www.kblockchain.org/board/press/read/116; Joon-Young Kim & Hyung-Seok Han, *Legal Issues and Self-Regulation Related to Cryptocurrency Transactions*, 89 BFL 50, 62 (Seoul National University Financial Law Center, 2018).

[33] Korean Block Chain Association *supra* note 32, at 1.

[34] *Id.* at 2.

exchanges to provide enough information to clients.[35] The KBCA will provide exchange information about problematic coins. Exchanges should use this information as part of the internal review process for listing new coins.[36]

While specific ICO regulation does not currently exist, the Korean government has acted to emulate international cryptocurrency standards. The FSC and the Financial Intelligence Unit,[37] a South Korean governmental agency in charge of anti-money laundering regulation, promulgated guidelines on money laundering in cryptocurrency transactions; the guidelines require account owner identification in all cryptocurrency trades.[38] Six months later, the FSC and the Financial Intelligence Unit amended the guidelines to improve transparency and strengthen monitoring in order to detect money laundering in cryptocurrency transactions.[39] Furthermore, on March 5, 2020, the Korean Congress passed the bill amending the Act on Reporting and Using Specified Financial Transaction Information to mandate cryptocurrency exchanges' anti-money laundering duties.[40]

---

[35] *Id.*

[36] *Id.* According to the framework, exchanges should protect investors' deposits by differentiating between exchange assets and investor deposits. In addition, exchanges should deposit 100 percent of the cryptocurrency to be prepared for clients' withdrawal requests. Moreover, the framework requires exchanges to run an electronic complaint center to promptly resolve clients' problems. Exchanges should establish an IT security system, internal processes, and sufficient human resources capacity.

[37] The Korea Financial Intelligence Unit, established in 2001,is responsible for the implementation of anti-money laundering laws and regulations as well as collecting, and analyzing suspicious transaction information to supervise and monitor for the compliance of financial companies with its regulations. *See* KOFIU, MESSAGE FROM THE COMMISSIONER, https://www.kofiu.go.kr/eng/intro/about.do.

[38] Before the Financial Information Unit guidelines were promulgated, cryptocurrency traders could have used virtual accounts as their trading accounts. This created a situation where the cryptocurrency traders' real names could not be easily detected. Some cryptocurrency traders even used one account which could be disguised as the operating capital account for a corporation. Current guidelines require traders to have a bank account with the same bank that the exchanges use to identify the account owner. Exchanges also need to identify traders' real names. In addition, multiple individual traders are prohibited from jointly using a corporate account. Financial Services Commission, *The Government Prepares Special Measures to Eradicate Virtual Currency Speculation* (Dec. 28, 2017), https://www.fsc.go.kr/no010101/72961?srchCtgry=&curPage=&srchKey=sj&srchText=&srchBeginDt=2017-12-23&srchEndDt=2017-12-31.

[39] The amendments include sharing overseas cryptocurrency dealer information. *See* Financial Services Commission, *Guidelines for Anti-Money Laundering Related to Virtual Currency* (June 27, 2018), https://www.fsc.go.kr/no010101/73223?srchCtgry=&curPage=2&srchKey=sj&srchText=&srchBeginDt=2018-06-24&srchEndDt=2018-06-30.

[40] This bill is still in effect as of March 2021. The Legal 500, *Amended Act on Reporting and Using Specified Financial Transaction Information Now Governs Virtual Assets*, (Mar. 13, 2020) https://www.legal500.com/developments/thought-leadership/amended-act-on-reporting-and-using-specified-financial-transaction-information-now-governs-virtual-assets/; This amendment includes the introduction of virtual asset concepts, several requirements for cryptocurrency exchanges such as certified information security management system. *See* Joon Young Kim, Samuel Yim & Jungmin Lee, *The Legal 500 Country Comparative Guides - South Korea: Blockchain*, THE LEGAL 500 (2020).

While the Korean government has taken a cautious approach to introduce the governmental framework to regulate cryptocurrencies, including ICOs, as of September 2019, there have been approximately ten legislative proposals submitted to the Korean Congress to regulate cryptocurrency or promote the blockchain industry.[41] Among the bills, Senator Taekyeong Ha's bill introduced a legislative proposal to amend electronic trading laws.[42] It requires ICO issuers to obtain approval for ICOs from the FSC. The ICO review committee within the FSC will consider approval according to the standards the FSC announced beforehand.[43] This ICO review committee consists of nine members including a chairman who is the FSC vice president.[44] The FSC has discretionary authority to cancel the ICO if: i) the approval is based on fraudulent methods; ii) such ICO is below the FSC standards; or iii) no transaction has occurred for more than one year.[45]

B. Problems

Since the Korean government announced several strong regulations, including banning ICOs in September 2017, it has taken few specific actions to enforce these regulations. The Korean government has kept a cautious stance toward regulating the cryptocurrency market, while it observes and researches regulations in other countries including the G20.[46] Possible reasons for doing so include the desire to not suppress potential market growth by excessive regulation; balanced with the desire to enact regulations strong enough to prevent the Korean market from becoming a playground for perpetrators of fraud.

In the meantime, cryptocurrency industries and investors have experienced chaos in different ways. First, the Korean government's ICO ban drove all ICO firms to conduct ICOs outside of Korea. In order to develop the Korean government's position toward ICOs, the Financial Supervisory

---

[41] YOUNGWOO SHIN, *Buleokcheinbeobeui Mirae* [*The Future of Blockchain Law*], *in* BULEOKCHEINGWA BEOB [BLOCKCHAIN AND LAW], 471, 482-83 (Kyeonghan Sohn ed., 2019).

[42] Proposal No. 15745, *Amendment of the Act on Electronic Transaction*, (Sept. 2, 2018) (repealed May 29, 2020, due to expiration of terms), https://likms.assembly.go.kr/bill/billDetail.do?billId=PRC_K1M8Z0M9X2L7E1H2S5P3N4H9V1V7Q.

[43] *Id*.

[44] *Id.* at 6-7, art. 38.5.

[45] *Id.*

[46] Financial Services Commission, *The Government Recognizes Some of the Virtual Currency Functions*, (May 28, 2018) https://www.fsc.go.kr/no010101/73176?srchCtgry=&curPage=&srchKey=sj&srchText=%EB%A8%B8%EB%8B%88%ED%88%AC%EB%8D%B0%EC%9D%B4&srchBeginDt=&srchEndDt= (responding to MONEYTODAY's article).

Service[47] investigated the ICO situation from September 2018 to November 2018, targeting twenty-two Korean companies that conducted ICOs.[48] According to the investigation, Korean ICO companies conducted ICOs outside of Korea by establishing shell companies that actually operated in Korea.[49] Korean ICO companies in Korea participated in all other aspects of the business such as project development and investor relations. Although it is called an overseas ICO, Korean investors consider the company to be a Korean ICO because the firms advertise to Korea and publish white papers in Korean. For example, BORA Systems launched an ICO in May 2018 at investors in both Hong Kong and Korea.[50] BORA Systems disclosed information about the project through a white paper both in Korean and in English. This was a typical pre-sale style ICO because it was performed while the company was developing platforms and other contents.[51]

Second, cryptocurrency fraud is causing vulnerable investors to suffer damages. According to FSA investigations, Korean ICO companies did not provide investors with important information they needed to make critical decisions, including financial information and project contents.[52] Many white papers, introductions, and profiles of developers failed to disclose or falsified vital information.[53] Significantly, most Korean ICO companies did not disclose how they used the funds from ICOs, and despite the FSA's requests, most of them failed to answer.[54] No company has launched service.[55] Rather, they are in the development or testing stage, but their progress information has not been disclosed either.[56] Project contents and Blockchain technology are not easy for the general public to understand. For investors who expected the gain from investing their money in ICOs, it

[47] The Financial Supervisory Service (FSS) is a quasi-governmental agency created to carry out the financial supervision delegated by the Financial Supervisory Commission (FSC). The FSC is responsible for rulemaking and licensing and the FSS is responsible for prudential regulations, enforcements, etc. *See* FINANCIAL SUPERVISORY SERVICE, HISTORY, https://english.fss.or.kr/fss/eng/wpge/eng111.jsp.

[48] *ICO Survey Results and Future Countermeasures*, *supra* note 30 (The targeting companies were selected based on newspaper articles, rumors, etc. Originally it was twenty-four companies but two of them gave up ICO).

[49] *Id*. at 3, 7. Those overseas shell companies were usually made up of less than three employees. Overseas shell companies usually do not hire new employees, and instead rely on employees from Korean ICO companies who also work for them. The capital was minimal, generally less than ten thousand dollars, and the shell companies only participated in fundraising activities. Those shell companies contracted with Korean ICO Companies, to which they then transferred the funds they raised.

[50] Linda Willemse, *Blockchain Based BORA Island (Mainnet) Releases BORA Lagoon (Testnet)*, MEDIUM (Nov. 9, 2018), https://medium.com/swlh/blockchain-based-bora-island-mainnet-releases-bora-lagoon-testnet-acccdb017174.

[51] *Id*.

[52] *ICO Survey Results and Future Countermeasures*, *supra* note 30.

[53] *Id*. at 2.

[54] *Id*.

[55] *Id*. at 3.

[56] *Id*.

was not a good choice because the prices of all newly issued coins dropped an average of 68% compared to the price of the first day of trading.[57]
Third, during the course of ICOs, ICO firms have violated current laws such as fundraising without registration under the FSCMA. In 2017, according to the dispute case analysis by FSA, more than 60% of illegal fundraising was related to ICOs.[58] The lack of clear guidelines made this situation worse. Therefore, it is important to examine how to regulate cryptocurrency under the FSCMA and eliminate the chaos.

Despite this turmoil, the clear regulation for ICO has not been introduced yet. The government keeps the static ban on ICOs. In a press release announcing the FSA Investigation, the Korean government showed worries that investors may misunderstand that the government authorizes illegal ICOs.[59] Ironically, although cryptocurrency technology and development through ICOs are key to developing the blockchain industry, the Korean government supports the development of the blockchain industry whilst banning ICOs.[60] Despite this government policy, according to FSA investigation, it seems that Korean ICO firms continue to conduct ICOs overseas,[61] causing the related frauds to continue occurring. Without creating the necessary regulatory regime on ICOs, merely banning ICOs cannot solve the problem.

If the Korean government wants to promote the blockchain industry, it should also promote ICOs. Instead of worrying about the side effects of the new regulation, it should suggest a method to distinguish between the good and the bad ICOs, and it should consider flexible regulation easily adaptable to the changing situations.

IV. GLOBAL RESPONSE

Attempts to develop proper ICO regulation is not unique to South Korea. This section will explore how other countries and other regional hubs have reacted to ICOs. It will specifically focus on the United States, Singapore, and Japan. These countries have all taken differing levels of scrutiny for regulating ICOs. This section will conclude by reflecting on these global approaches to ICO regulation and will draw lessons for potential South Korean ICO regulation.

---

[57] *Id*. at 8. Average 68% down, compared the price of the first trading day with the price at the end of 2018. Profit Ratios are all negative, between negative 15% to 96.

[58] Kwan Hyung Lee, *Amhohwapyeo gwanryeon beomjeoui gusaegwanhan heongsajeongcheokjeg gochal – cheogeun gukheoibbeoneonuirul gungsimeuro* [*Review on Prevention and Investigation of Cryptocurrency-related Crimes from the Criminal Justice Perspective*] 19 GYEONGCHALHAKYEONGU [J. POLICE SCI.] 63, 73 (2018).

[59] *ICO Survey Results and Future Countermeasures*, *supra* note 30.

[60] *Id*.

[61] *Id.* at 3, 7; *see also* Yogita Khatri, *South Korea Will Maintain ICO Ban After Finding Token Projects Broke Rule*, COINDESK (Jan. 31, 2019), https://www.coindesk.com/south-korea-will-maintain-ico-ban-after-finding-token-projects-broke-rules.

A. United States

In the case of U.S. regulations, many utility tokens could be classified as security tokens if they have an investment function. The Securities & Exchange Commission ("SEC") in the U.S. started applying the *Howey* standard to cryptocurrency. Still, the criteria to distinguish between security tokens and utility tokens are not clear.[62]

i. The *Howey* Test

The U.S. Securities and Exchange Commission ("SEC") regulates ICOs by applying existing securities laws to cryptocurrencies, without creating new crypto-specific regulations.[63] In July 2017, in the DAO[64] No

[62] U.S. regulation on cryptocurrency started in early 2013. Financial Crime Enforcement Network (FinCEN) issued interpretive guidance to apply anti-money laundering (AML) regulation to cryptocurrency transactions. *See* Financial Crimes Enforcement Network (FinCEN), *Application of FinCEN's Regulations to Persons Administering, Exchanging, or Using Virtual Currencies*, (Mar. 18, 2013), https://www.fincen.gov/resources/statutes-regulations/guidance/application-fincens-regulations-persons-administering. Under this guidance, cryptocurrency exchanges should register their business, develop the compliance system, and reporting issues to FinCEN. *See* Kenneth A. Blanco, Prepared Remarks of FinCEN Director Kenneth A. Blanco, Delivered at the 2018 Chicago-Kent Block (Legal) Tech Conference (Aug. 9, 2018), https://www.fincen.gov/news/speeches/prepared-remarks-fincen-director-kenneth-blanco-delivered-2018-chicago-kent-block. Among states, New York is leading the regulation by creating a licensing regime for cryptocurrency business so called "BitLicense" in 2014. BitLicense set the comprehensive regulation for cryptocurrency exchanges including capital requirement and compliance programs in order to prevent frauds and money laundering. *See* New York State Department of Financial Services, 23 N.Y.C.R.R. 200.3(a) (2015) https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/regulation_history (last visited May 29, 2021); *see also* NEW YORK STATE DEPARTMENT OF FINANCIAL SERVICES, *VIRTUAL CURRENCY: BITLICENSE FAQ*, https://www.dfs.ny.gov/apps_and_licensing/virtual_currency_businesses/bitlicense_faqs (last visited May 29, 2021).

[63] Regarding derivatives regulation, in 2015, the Commodity Futures Trading Commission ("CFTC") applied the Commodity Exchange Act to Bitcoin and other cryptocurrencies. Coinflip, Inc., CFTC Docket No. 15-29, 2015 WL 5535736 (Sept. 17, 2015). In 2017, The CFTC allowed CME and CBOE futures exchange to carry derivative products whose underlying products are cryptocurrency by self-certifying process where exchanges certify compliance with laws. LABCFTC, A CFTC PRIMER ON VIRTUAL CURRENCIES (Oct. 2017), https://www.cftc.gov/sites/default/files/idc/groups/public/documents/file/labcftc_primercurrencies100417.pdf.

[64] The DAO, or Decentralized Autonomous Organizations, was developed by a German startup, Slock.it, which attempted to create business organizations or corporations by utilizing blockchain technology, Etherium and in April 2016, it created an "automated investment fund" for ICOs. If investors send Ether, the second-generation cryptocurrency, to DAO's account, then investors will receive DAO tokens. The DAO management runs the DAO project and gave token holders limited voting rights and dividend rights like stocks. SEC found the DAO meet the Howey test because the DAO runs projects and toke holders are promised a return on their investment. *See* SEC, *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934; The DAO* (July 25, 2017), https://www.sec.gov/litigation/investreport/34-81207.pdf; Usha Rodrigues, *Law and the*

Action Letter, the SEC declared that tokens were investment contracts under Section 2 of the Securities Act, and an issuer should comply with U.S. securities regulations, including the registration requirement.[65]

The *Howey* test, developed from *SEC v. W.J. Howey Co.*, defines an investment contract.[66] It consists of four prongs: (i) is there an investment of money; (ii) is there a common enterprise; (iii) is there a reasonable expectation of profits from the investment; and (iv) does the investment income solely from efforts of others.[67] First, there should be an investment of money. Recently a U.S. court held that payment with Bitcoin satisfies this prong, so there would be little dispute that ICOs would meet this requirement.[68] Second, there should be a common enterprise. Most courts adopt horizontal commonality.[69] Horizontal commonality exists when pooling assets and profit sharing exist.[70] In some ICOs, firms pooled funds and shared profits.[71] Third, there should be a reasonable expectation of profits.[72] According to the U.S. Supreme Court, there would be no expectation of profits if personal consumption is the purchaser's main motivation.[73] Thus, if the projects from ICOs are to buy some items for consumption, then there is no expectation of profits.[74] Fourth, investment should be solely from the efforts of others.[75] This depends on "whether efforts made by those other than the investor are the undeniably significant ones."[76]

The SEC determined that a token of the DAO project is a security based on the facts and circumstances. Under the *Howey* test analysis, investors *reasonably expected the profits* from the DAO project because the DAO was created as a for-profit entity that devotes investor funds raised for the DAO project; thus, investors expected to receive returns.[77] Also, this investment was *solely from the efforts of others* because managers of the

---

Blockchain, 104 IOWA L. REV. 679 (2018), https://digitalcommons.law.uga.edu/cgi/viewcontent.cgi?article=2274&context=fac_artchop.

[65] *Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934; The DAO*, *supra* note 64.

[66] SEC v. W.J. Howey Co., 328 U.S. 293, 301 (1946).

[67] *Id.*

[68] SEC v. Shavers, No. 4:13CV-416, 2014 WL 12622292, at 1 (E.D. Tex. Aug. 26, 2014).

[69] A minority of court apply a vertical commonality test instead of horizontal commonality test. *See* Juan Baltz-Benet, Marco Santori & Jesse Clayburgh, *The SAFT Project: Toward a Compliant Token Sale Framewor*k, COOLEY, at 7, (Oct. 2, 2017) https://saftproject.com/static/SAFT-Project-Whitepaper.pdf.

[70] Baltz-Benet, et. al., *supra* note 69 at 7; SEC v. SG Ltd., 265 F.3d 42, 49-50 (1st Cir. 2001).

[71] *SEC v. SG Ltd*., 265 F.3d 52.

[72] Choi & Pritchard, *supra* note 2, at 129-30.

[73] United Housing Foundation, Inc. v. Forman, 421 U.S. 837 (1975).

[74] William Hinman, *Digital Asset Transactions: When Howey Met Gary (Plastic*), SEC (June 14, 2018), https://www.sec.gov/news/speech/speech-hinman-061418.

[75] Choi & Pritchard, *supra* note 2 at 129-30.

[76] SEC v. Glenn W. Turner, 474 F.2d 476, 482 (9th Cir. 1973).

[77] *See Report of Investigation Pursuant to Section 21(a) of the Securities Exchange Act of 1934; The DAO*, *supra* note 64.

DAO control the management of the project.[78] Thus, the SEC decided that the issuer of the DAO token should comply with securities regulations, which includes registration requirements of issuers and exchanges.[79]

The *Howey* test protects investors widely and is flexible enough to cover every case. However, these flexibilities incur huge compliance costs to deciding whether the *Howey* test applies case by case. Many people from the industry would not understand implications of the *Howey* test clearly. More importantly, according to the *Howey* test, most utility tokens can possibly fall into the investment contract category, unless those utility tokens are clearly designed to purchase items for personal consumption. Even investment features can exist in those tokens issued for consumption of items if there is a secondary market for resale of those tokens.[80] The application of the *Howey* test may suppress ICOs, making them more difficult because people have to decide whether each ICO falls into the investment contract category. The SEC's approach of relying on the *Howey* test to analyze ICOs seems to be aligned with the philosophy of market regulation to strengthen investor protection. However, the *Howey* test's case by case application creates additional ambiguity in regulation.

On April 3, 2019, the SEC announced guidelines on ICOs intended to address these issues and help the public better understand the application of the *Howey* test to ICOs.[81] Although this guideline is not a legally binding opinion, it provides an analytical tool for ICO regulation.[82] The guideline states that in applying the *Howey* test on ICO, the investment of money and common enterprise requirements are typically met.[83] The more difficult hurdle is to maintain a reasonable expectation of profits derived from efforts of others. The guideline identifies features of ICOs that most likely and least likely satisfy this reasonable expectation of profits derived from the efforts of others requirement.[84] The guidelines elaborate on features that fail the expectation test, such as stating that "distributed ledger network and digital asset are fully developed and operational" or "prospects for appreciation in the value of the digital asset are limited."[85] Although it is not legally binding,

---

[78] *Id*. at 11-17, The DAO token holders have the voting rights, but they are limited to the proposal made by the manager, so basically investors did not control the DAO.

[79] *Id*. at 17-18.

[80] Brady Dale, *What If the SEC Is Going After the SAFT?,* COINDESK (March 6, 2018), https://www.coindesk.com/sec-going-saft.

[81] SEC, *Framework for "Investment Contract" Analysis of Digital Assets* (April 3, 2019), https://www.sec.gov/ICO.

[82] Bill Hinman & Valarie Szczepaik, Statement on Framework for 'Investment Contract' Analysis of Digital Assets (April 3, 2019) https://www.sec.gov/news/public-statement/statement-framework-investment-contract-analysis-digital-assets.

[83] *Framework for "Investment Contract" Analysis of Digital Assets*, *supra* note 81.

[84] *Id.*

[85] *Id.*

the guideline clarifies investment contract requirements and guides compliance.[86]

In the meantime, the SEC issued a No Action Letter to an ICO firm where the ICO does not satisfy the *Howey* test. On April 10, 2019, the SEC issued a No Action Letter to TurnKey Jet, Inc. where TurnKey Jet plans to tokenize gift cards only for its members.[87] According to SEC's analysis, the first prong, investment of money, exists because investors paid funds to buy tokens.[88] However, the second prong, common enterprise, does not exist because investors use the tokens for their intended purpose like prepaid services but did not expect returns.[89] Also, the third prong, expectation of profit, also does not exist because investors do not have the rights for returns, dividends, etc., even though they buy the service more efficiently by purchasing tokens.[90] There are few features of investment because the issuer already fully developed the platform before ICO and the issuer did not emphasize the investment features.[91] In these regards, the *Howey* test is not met. Applying the *Howey* test to ICOs is still challenging, but the SEC has proceeded to clarify regulation with these efforts.

ii. Simple Agreement for Future Tokens

The *Howey* test is flexible, but its requirements make it harder for ICO firms to raise funds, and ambiguity still exists despite SEC guidelines. To avoid the ambiguity of the *Howey* test, many U.S. ICO teams use a Simple Agreement for Future Tokens ("SAFT") to ensure that registration requirements are waived relying on exemption mechanisms under securities regulations. In the SAFT, ICO firms direct offers only to accredited investors who qualify for private sale.[92] They acknowledge that the SAFT is "very likely" to be regarded as an investment contract under the Securities Act, thus ICO firms will rely on an exemption from regulation requirement based on Regulation D.[93] They usually rely on Rule 506(c) of the Regulation D under the Securities Act, where companies can raise funds without limitation.[94]

---

[86] Nikhilesh De, *The SEC Just Released Its Long-Waited Crypto Token Guidance*, COINDESK (April 3, 2019), https://www.coindesk.com/the-sec-just-released-its-crypto-token-guidance.

[87] Commissioner Hester M. Pierce, Sec. & Exch. Comm'n, How We Howey (May 9, 2019), https://www.sec.gov/news/speech/peirce-how-we-howey-050919.

[88] SEC, *Response of the Division of Corporation Finance Re: TurnKey Jet, Inc.*, at 9 (April 3, 2019) https://www.sec.gov/divisions/corpfin/cf-noaction/2019/turnkey-jet-040219-2a1.htm.

[89] *Id.* at 10.

[90] *Id.*

[91] *Id.* at 12.

[92] Juan Baltz-Benet et al., *supra* note 69, at 16 n.69.

[93] *Id*. at 15.

[94] *Id*. at 16. Issuers can sell securities to accredited investors without limitation and to thirty-five other investors. Purchasers of these securities have resale restrictions for six months. 17 CFR §230.506; Rule 506 of Regulation D, SECLAW.COM, https://www.seclaw.com/sec-rule-506/.

Usually after ICO firms raise funds, they develop the platform and deliver the tokens to investors.[95] The investors then resell tokens to the public.[96] A benefit of the SAFT model is that the general public can avoid the risk of the project defaulting in addition to enjoying the investor protection of securities regulation.

However, because the SAFT is designed for resale purposes, not the consumption of items, this mechanism can be used to avoid regulation.[97] Reflecting this concern, the U.S. courts made a decision that if the initial purpose of ICO was to distribute tokens, then such sales cannot enjoy exemption from securities regulation.[98] In *SEC v. Telegram Group Inc.*, the court said that the economic reality is important regardless of the fact that sales were made to sophisticated investors.[99] Thus, ICO firms cannot enjoy safe harbor relying on SAFT.

Overall, the U.S. government has put a heavy burden on ICO firms, intended to protect investors. Despite this strong regulatory stance, ICO firms are adjusting to the regulatory status of ICOs. They have navigated to find legitimate ways to do ICOs such as through the SAFT. The U.S. courts also responded to prevent abuse of such measures by its ruling in *Telegram Group*. The next section will explore how Singapore, where many Korean ICO firms are housed, set up its regulatory framework for ICOs.

B. Singapore

Because the Chinese government and Korean government banned ICOs, the demand for ICOs is moving towards Singapore – making it the hub of ICOs in Asia.[100] In August 2017, the Monetary Authority of Singapore ("MAS") clarified that it would apply the Securities Futures Act, a securities regulation in Singapore, to cryptocurrency if the offer or issue of cryptocurrency constitutes a security or futures contract under the Securities Futures Act.[101] So if the cryptocurrency is offered or sold for economic

---

[95] Juan Baltz-Benet et al., *supra* note 69 at 18.

[96] *Id*.

[97] Authors also point out this as one of limitation of SAFT. *Id.* at 20.

[98] SEC v. Telegram Group Inc., No. 1:19-cv-09439-PKC, 38 (S.D.N.Y. Mar. 24, 2020).

[99] *Id.* at 42.

[100] According to ICO rating, an ICO rating agency, in the first quarter of 2018, Singapore is ranked in second to U.S. in the number of ICO offering and the first ranked in Asia. ICO Rating, *ICO Market Research Q1 2018*, https://icorating.com/ico_market_research_q1_2018_icorating.pdf; *See also* NEWSBTC, *Hong Kong and Singapore Welcome Chinese and South Korean ICOs*, (April 23, 2018), https://www.newsbtc.com/2018/04/23/hong-kong-singapore-welcome-chinese-icos.

[101] Monetary Authority of Singapore, *MAS Clarifies Regulatory Position On The Offer of Digital Tokens in Singapore*, (August 1, 2017), https://www.mas.gov.sg/news/media-releases/2017/mas-clarifies-regulatory-position-on-the-offer-of-digital-tokens-in-singapore; Before this action, in March 2014, MAS announced that cryptocurrency would be regulated, focusing on potential money laundering and terrorist finance risks. MAS reasoned that due to the anonymous nature of the transactions, cryptocurrency is more vulnerable to money

benefits such as dividends, that cryptocurrency will be regulated as a security, a collective investment scheme, or sometimes a debenture under the Securities Futures Act.[102] MAS emphasized that in that case, issuers of those tokens should comply with the disclosure requirement, unless exempt.[103] Also, unless exempt, issuers or intermediaries of tokens should obtain license under the Securities Futures Act and Financial Advisers Act.[104] Exchanges also should be approved or recognized by MAS under the Securities Futures Act.[105]

To elaborate on this ICO regulation, in November 2017, MAS issued "a Guide to Digital Token Offering" ("Singapore Guideline") and explained ICO regulations in a detailed manner, including exemptions and exemplifying cases.[106] Case studies in the Singapore Guideline exemplify the cases where tokens issued in ICOs can be regarded as shares, a Collective Investment Scheme, or a debenture.[107] Also, it elaborated cases where regulation does not apply, such as a payment token offering to foreigners.[108]

ICO status does not seem to be affected by these strengthened regulations. According to ICO Rating's quarterly report of 2018, the second quarter's ICO performance in Singapore increased 23% in terms of capital size, 68% in terms of number of cases compared to first quarter.[109] Also the 2018 semi-annual performance in Singapore increased 263% in terms of capital size, 219% in terms of number of cases compared to the 2017 semi-annual performance.[110] This growth is similar to the growth of the other four

---

laundering and terrorist finance risks. Monetary Authority of Singapore, *MAS to Regulate Virtual Currency Intermediaries for Money Laundering and Terrorist Financing Risks*, (Mar. 14, 2014) ,https://www.mas.gov.sg/news/media-releases/2014/mas-to-regulate-virtual-currency-intermediaries-for-money-laundering-and-terrorist-financing-risks.

[102] Securities and Futures Act, Ch. 289, (April 1, 2006) https://sso.agc.gov.sg/Act/SFA2001.

[103] *MAS Clarifies Regulatory Position On The Offer of Digital Tokens in Singapore*, *supra* note 101.

[104] *Id.*

[105] *Id*.

[106] Monetary Authority of Singapore, *A Guide to Digital Token Offerings*, 2 (May 26, 2020), https://www.mas.gov.sg/regulation/explainers/a-guide-to-digital-token-offerings. The offer to sell tokens in ICOs should comply with the requirements of Part XIII of Securities Futures Act including prospectus registered with MAS and accompanied with the offer. Some cases such as the offer made to institutional investors enjoy the exemption from these requirements as elaborated in 2.6 of the guideline.

[107] *Id.*

[108] *Id*. Under this policy, in May 2018, MAS warned eight cryptocurrency exchanges to seek MAS approval in order to facilitate trading of cryptocurrency which falls into the securities or futures contract under the Securities Futures Act. Also, MAS directed one ICO issuer to stop its ICO in Singapore. The issuer argued that its token represents the equity ownership of the company, so it falls into the category of securities and futures product, but it was not registered MAS and distributed without prospectus.

[109] ICO RATING, ICO MARKET RESEARCH Q2 2018, https://icorating.com/report/ico-market-research-q2-2018/.

[110] ICO RATING, ICO RATING ANNUAL REPORT 2017, https://icorating.com/report/icorating-annual-report-2017/.

major countries (i.e. United States, United Kingdom, Switzerland, Estonia) in ICO offerings. Presumably, many market participants are from neighboring countries such as China and Korea, which adopted the strong regulation such as banning ICOs.[111] The decision to strengthen the regulation was made right after the U.S. SEC announced that it will apply securities regulation to ICOs. The strengthening regulation seems to work as a good sign for the ICO market. Most ICO markets do not have clear regulations, which makes ICO firms and investors unpredictable. Singapore regulators seize the core problem and propose clear regulations, which encourages predictable and stable markets that benefit market participants. Also, ICO demands from companies originated in China and Korea seem to go to Singapore with its strong financial center, making Singapore's ICO market much stronger.

To guarantee the flexibility of regulations related to the fintech industry, MAS has run the FinTech Sandbox since 2016.[112] Any companies having regulatory concerns regarding cryptocurrency, including ICOs, can apply to MAS for the Fintech Sandbox. Once an application received, MAS determines the eligibility by seven evaluation criteria, such as innovative characteristics of financial service.[113] So far, this research has explored U.S. and Singapore which dominate ICOs in their respective region and their regulations are clear and strong. In the following subsection, the research will examine Japan which has started to introduce new regulations on ICOs.

---

[111] Singapore was not the dominant country in country of fund origin but it is the leading country in ICO registration. ICO RATING, ICO MARKET RESEARCH Q1 2018, https://icorating.com/ico_market_research_q1_2018_icorating.pdf.

[112] Monetary Authority of Singapore, *FinTech Regulatory Sandbox Guidelines*, 6.2 (Nov. 2016); *see also* Monetary Authority of Singapore, *MAS Proposes a "Regulatory Sandbox" for FinTech Experiments* (June 6, 2016), https://www.mas.gov.sg/news/media-releases/2016/mas-proposes-a-regulatory-sandbox-for-fintech-experiments#:~:text=3%20The%20regulatory%20sandbox%20will,well%2Ddefined%20space%20and%20duration.The Singaporean government plans to build the Smart Financial Center in Singapore, and to support the government plan, MAS set up a new financial innovation support group (FinTech & Innovation Group) inside MAS in July, 2015.

[113] *FinTech Regulatory Sandbox Guidelines*, *supra* note 112. Elaborates on seven evaluation criteria to determine whether an applicant is eligible for the FinTech Sandbox as follows:

Is the proposed financial service innovative?
Does the proposed financial service address a problem, bring benefits to customers or industry?
Does the applicant have the intention and ability to use the proposed financial service in Singapore on a broader scale after exiting the sandbox?
Are the test scenarios and outcomes of experiments clearly defined?
Is the appropriate boundary conditions clearly defined?
Are significant risks arising from the proposed financial services assessed and mitigated?
Is the acceptable exit and transition strategy clearly defined?

C. Japan

Japanese cryptocurrency regulations began as a response to issues with cryptocurrency's use as a payment method. In 2014, Mt. GOX, a Japanese cryptocurrency exchange starting to operate from 2010, claimed insolvency resulting from the theft of its Bitcoins by insiders manipulating.[114] In 2016, The Japanese Financial Services Agency (FSA) responded by creating "the Cryptocurrency Act."[115]

Also, the FSA amended the Payment Services Act, which became effective on April 1, 2017.[116] Under the Payment Service Act, cryptocurrency is defined as a currency.[117] In January 2018, Coincheck lost cryptocurrencies worth 500 million dollars in a hack caused by a poor security system.[118] In response, sixteen exchanges created the self-regulation organization known as the Japanese Virtual Currency Exchange Association ("JVCEA") to address the cryptocurrency market adequately.[119]

As investor interests have focused on ICOs, regulators' focus also started to shift to ICOs. In 2018, a private study group was formed; it consisted of representatives from financial companies, IT companies, and the government.[120] It issued a report about principles and guidelines for

---

[114] Mt.Gox is known to occupy around 70% of Bitcoin transactions at its peak time. Jake Frankenfield, *Mt. Gox*, INVESTOPEDIA, (Mar. 26, 2021) https://www.investopedia.com/terms/m/mt-gox.asp.

[115] Library of Congress, *Regulation of Cryptocurrency: Japan*, http://www.loc.gov/law/help/cryptocurrency/japan.php#VII.

[116] *Id.*

[117] Payment Services Act No. 59, art. 2(5), (June 24, 2009) translated in [Japanese Law Translation] http://www.japaneselawtranslation.go.jp/law/detail/?id=3078&vm=02&re=02.

[118] BBC NEWS, *Coincheck: World's Biggest Ever Digital Currency 'Theft'* (Jan. 27, 2018) https://www.bbc.com/news/world-asia-42845505.

[119] Pushpa Naresh, *Japan's FSA Sets Up JVCEA to Regulate and Set Up Policies for Crypto Exchanges*, NEWCONOMY (Nov. 2, 2018), https://newconomy.media/news/japans-fsa-sets-up-jvcea-to-regulate-and-set-up-policies-for-crypto-exchanges. JVCEA is making efforts to create best practice and compliance standards and advise unlicensed exchanges. Ryan Clements, *Can a Cryptocurrency Self-Regulatory Organization Work? Assessing Its Promise and Likely Challenges*, THE FINREG BLOG, (June 21, 2018), https://sites.law.duke.edu/thefinregblog/author/ryan-clements/. JVCEA proposed the self-regulatory rules, including a ban on insider trading, margin limits and caps, and applied for FSA's approval as a self-regulatory organization to enforce its regulation. Kevin Helms, *Japanese Association Seeks Authority to Enforce Self-Regulation on Crypto Exchange*, BITCOIN.COM, (Aug. 3, 2018), https://news.bitcoin.com/japanese-association-self-regulation-crypto-exchanges.

[120] ICO Business Research Group, *Call for Rule-making on ICO*, CENTER FOR RULE-MAKING STRATEGIES AT TAMA UNIVERSITY, 1 (April 5, 2018) https://www.tama.ac.jp/crs/2018icoen.pdf.

legalizing ICO ("the ICO Report").[121] The ICO Report proposed two principles and two guidelines for issuance and five guidelines for trading.[122]

First, the two principles for issuance recommend that issuers clearly disclose ICO conditions and the progress of the project in a white paper to investors. Issuance Principle #1 requires issuers to clearly disclose ICO conditions to investors, shareholder, and debtholders.[123] Issuance Principles #2 requires issuers to disclose the progress of ICO plans in a white paper.[124] The ICO Report focuses on innovations and flexibility in ICOs as well as investor protections.[125] As guidelines for operations, the ICO Report suggests that the design of ICOs should be "acceptable to existing shareholders and debtholders and should not become a loophole in existing financing methods as equity finance."[126]

Second, to ensure appropriate investor protection, the ICO Report proposes five principles for purchase and sale of cryptocurrency. It includes "Know Your Customer" rules, listing rules, and unfair practice rules.[127] After the hacking of Coincheck, the FSA recognized that the then-current regulatory regime was inadequately protecting investors in case of an exchange's bankruptcy. Therefore, to strengthen investor protection the FSA organized a study group on legalizing the ICO in April 2018.[128] This regulatory change would alter the concept of cryptocurrency from a payment method to a financial product.[129]

---

[121] Yuki Hagiwara et. al., *Japan Unveils Guidelines for Allowing Initial Coin Offerings*, BLOOMBERG (April 4, 2018); *See also* ICO Business Research Group, *Call for Rule-making on ICO*, CENTER FOR RULE-MAKING STRATEGIES AT TAMA UNIVERSITY, 1 (April 5, 2018) https://www.tama.ac.jp/crs/2018_ico_en.pdf.

[122] *Call for Rule-making on ICO*, *supra* note 120 at 1.

[123] *Id.* at 4-5.

[124] *Id.* at 5.

[125] *Id*. at 4.

[126] *Id*. at 5.

[127] *Id*. at 5-6. Trading principles as follows:

Trading Principle 1: Token Sellers should confirm the identity (Know Your Customer: KYC) and suitability of customers.

Trading Principle 2: Administrative companies that support the issuance of tokens should confirm the KYCs of issuers.

Trading Principle 3: Cryptocurrency exchanges should define and adopt an industry-wide minimum standard on token listing.

Trading Principle 4: After tokens are listed, unfair trade practices of such tokens such as insider trading should be restricted.

Trading Principle 5: Parties related to the trading of tokens such as issuers, administrative companies, and token exchanges should make efforts to ensure cyber security.

[128] Financial Services Agency, *About the Establishment of "Study Group on Virtual Currency Exchange Business, etc."*, (Mar. 8, 2018), https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181228.html.

[129] Financial Services Agency, *Report from Study Group on Virtual Currency Exchange Services*, 1 n. 2 (Dec. 21, 2018) https://www.fsa.go.jp/en/refer/councils/virtual-currency/20181221-1.pdf.

In December 2018, the FSA announced its study report, including the new ICO regulation proposal.[130] In this report, the FSA classified the ICOs into three groups: Investment Type, Other Rights Type, and Unprivileged Type.[131] Investment Type means the ICOs firms promise the future distribution of profits.[132] The Other Rights Type is an ICO in which the firm promises to provide services and material.[133] The Unprivileged Type is the ICO type in which the firm do not have any obligations to investors like a donation.[134]

In this report, the FSA says that the Japanese securities regulation, the Financial Instrument and Exchange Act (Financial Act), should apply to the Investment Type ICO.[135] The Payment Act should apply for the Other Rights Types.[136] The FSA describes the following as features of Investment Type ICO: (i) high freedom of token design; (ii) high information asymmetry between ICO firms and investors; and (iii) recruiting investors through the internet, which makes raising funds easier but recognizing frauds harder.[137] The FSA argues that these characteristics cause more risks to investors, so regulators should create the measures to control them.[138] Because tokens can be distributed easily like securities and be a target of fraud, the FSA proposed the following regulations: (i) more disclosure to reduce information asymmetry; (ii) screening by a third party, such as securities firms to prevent the fraud; (iii) unfair trading regulation such as price manipulation; and (iv) limiting the secondary market, such as limiting sale to only accredited investors.[139]

Based on these discussions, the Japanese government proposed to regulate securities type tokens like securities. It amended the Payment Act and Financial Act on May 31, 2019, which became effective on May 31, 2020.[140] By these amendments, the Japanese government introduced "electronic transfer right (*denshi kiroku iten kenri*)," so tokens with securities features will be regulated by the Financial Act and will therefore have

---

[130] *Id*. at 1.
[131] *Id*. at 20.
[132] *Id*.
[133] *Id.* at 20, 27. For Other Rights Types where the FSA applies settlement regulation, the FSA emphasizes the role of exchanges and collaboration of the government and the self-regulators. Exchanges should require ICOs firms to provide investors the financial status of ICOs firms, the foundation of the price of tokens, and the feasibility and progress of the project.
[134] *Id*. at 20.
[135] *Id*.
[136] *Id*. at 21.
[137] *Id*. at 22.
[138] *Id*.
[139] *Id*. at 22.
[140] Youngeun Cho, *Strengthening Protection Regulation of Cryptoasset Users in Japan, Foreign Legislation: Trends and Analysis*, NATIONAL ASSEMBLY RESEARCH SERVICE, vol. 38, (April 19, 2019). https://www.nars.go.kr/eng/report/view.do?page=67&cmsCode=CM0136&categoryId=&searchType=&searchKeyword=&brdSeq=25468.

registration and disclosure duties.[141] However, if the offering meets some conditions such as being limited to Qualified Institutional Investors, then regulation, such as the registration requirement, will be eased.[142] Thus far, this paper has examined the regulatory response of United States, Singapore and Japan. The next subsection will reflect the response and draw insights to Korean ICO regulation.

D. Reflection on Research of Global Regulation

Every country has its own way to regulate cryptocurrency—and nearly every country discussed herein is starting, or preparing to start, applying securities regulation regimes to ICOs. This approach has become a global trend for investor protection. Security tokens and utility tokens under certain circumstance may be regulated as securities. However, as noticed in the U.S., it is not simple to apply securities regulation to utility tokens. The standard to define security features and application of rules vary by country. Many utility tokens with securities features may be treated as securities. But applying securities regulation to utility tokens with no securities features will incur huge social costs including administrative cost of the government and compliance cost of issuers. It also creates additional ambiguity in regulation by applying securities regulation case by case.

To solve these problems, regulators have provided guidelines to distinguish features of securities token and utility tokens. The U.S. SEC Guidelines exemplify features of utility token cases with "distributed ledger network and [where] digital asset are fully developed and operational" or "prospects for appreciation in the value of the digital asset are limited."[143] The Singapore Guideline elaborates cases of utility tokens where no rights or functions are attached to tokens other than real use right of platform.[144] In the study report, Japanese FSA focuses more on the features of securities token. It describes features for security token and includes cases that i) the information asymmetry for such token is great, ii) ICO was based on internet

---

[141] *See* Tsuguhito Omagari and Yuki Sako, *Japan's New Crypto Regulation: 2019 Amendments to Payment Services Act and Financial Instruments and Exchange Act of Japan*, K&L GATES, (Nov. 26, 2019), https://www.klgates.com/Japans-New-Crypto-Regulation-2019-Amendments-to-Payment-Services-Act-and-Financial-Instruments-and-Exchange-Act-of-Japan-11-26-2019. Main contents of these amendments include name changes of virtual currency to currency assets, crypto asset derivative regulation, and unfair trading regulation. *See also* Sygna, *Japan's Financial Services Agency (FSA) to Enforce New Crypto-Asset Exchange Regulations from 1 May 2020*, https://www.sygna.io/blog/japan-crypto-asset-regulation-financial-services-agency-changes-psa-fiea-may-2020/.

[142] Clifford Change, *New Regulations for Crypto-Assets (Virtual Currencies) and Initial Coin Offerings and Security Token Offerings in Japan*, (Feb. 2020), https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2020/02/New-Regulations-for-Crypto-Assets-(Virtual-Currencies)-and-Initial-Coin-Offering%20-and-Security-Token-Offering-in-Japan.pdf.pdf.

[143] SEC, *Framework for "Investment Contract" Analysis of Digital Assets*, (April 3, 2019), https://www.sec.gov/corpfin/framework-investment-contract-analysis-digital-assets.

[144] *FinTech Regulatory Sandbox Guidelines*, *supra* note 112 at 14.

so ICO firms easily approach investors, or iii) high degree of design freedom for ICO firms exist.[145] As discussed above, the global regulators examined in this Article already applied, or have started to apply, a securities regulations regime to security tokens. To provide investors and ICO firms with information on how to distinguish between security tokens and utility tokens, each country's regulators are making efforts to build up guidelines.

Additionally, it is noticeable that the U.S. and Singapore have strong and clear regulatory regimes. Especially, in the case of Singapore, although MAS introduced stronger regulations, it did not influence ICO performance and rather, clearer regulation played as a good sign for ICO demands. Also, flexibility of regulation is important considering features of ICOs and tokens. The cryptocurrency industry is rapidly developing. The U.S. and Singapore, both successful ICO hubs, use flexible regulations.[146]

In Singapore, ICO firms can ask for the FinTech Sandbox and MAS in Singapore will decide their eligibility case by case and if approved, they will enjoy exemptions from some of regulations.[147] This is flexible regulation that can fit every situation, but it may require high administrative cost and more human capacity for regulation. Regulators utilize disclosure regulation and third-party review to guarantee flexibility of regulation. It is also notable that FSA in Japan launched to regulate ICOs with security features with securities regulation.

In sum, application of securities regulation is becoming the global trend. Clear and flexible regulations are the key to developing the successful ICOs. To protect investors, disclosure and third-party review are preferable. In the next section, this Article proffers regulatory proposals for Korean ICO regulations.

V. REGULATORY PROPOSAL FOR ICO REGULATION IN KOREA

This section will propose future ICO regulations which could be implemented in Korea. The largest regulatory question today in Korea and globally is how to protect vulnerable investors through ICO regulation. Regulators must consider the economic cost and benefit of the legislation and the features of the industry when creating the new regulatory regimes. In this context, this section proposes using the existing securities regulation regime and strengthening disclosures. Also, this Article proposes limiting ICO participants by relying on crowdfunding laws or SAFT. Lastly, considering

---

[145] ICO Business Research Group, *Call for Rule-making on ICO*, CENTER FOR RULE-MAKING STRATEGIES AT TAMA UNIVERSITY, 4-5, (April 5, 2018) https://www.tama.ac.jp/crs/2018_ico_en.pdf.

[146] SEC v. Howey Co., 328 U.S. 293 (1946). As described in III. Global Response, U.S. relies on the flexible *Howey Test* to decide whether ICOs fall into the purview of securities regulation case by case.

[147] *FinTech Regulatory Sandbox Guidelines*, *supra* note 112 at 10.

that the cryptocurrency ecosystem is quickly growing, regulators should also focus on keeping regulations flexible.

A. Korea Should Regulate ICOs under Existing Securities Law Rather than Creating New Regulations

The Korean government should consider using the current securities regulation regime to regulate ICOs, rather than creating new legislation.[148] Although ICOs and IPOs are different, they function similarly to fund companies for projects. Concerns regarding investor protections are present in both ICOs and IPOs. Under the principle of "the same economic function, the same regulation," regulators can consider using securities regulation to regulate ICOs.[149] By regulating ICO with FSCMA, the government can take advantage of the pre-existing regulatory schemes such as disclosure requirements to protect investors.[150]

Moreover, this can reduce the high cost of administration. Out of approximately ten bills covering cryptocurrency proposed by the Korean Senate as of September 2019, only three bills proposed creating new laws, while the others proposed amending current law.[151] However, all bills were repealed and the bills amending the Act on Reporting and Using Specified Financial Transaction Information were approved with the alternative bills proposed by the National Policy Committee in March 2020.[152]

That failure to legislate contributes to the delay of regulation, causing investors vulnerable to ICO-related frauds. If the government used the current securities regulation regime, it could save this legislative burden and introduce an operative regulatory framework quickly and easily. The Korean government can rely on investor protection mechanism of the FSCMA such as disclosures.[153]

Moreover, as discussed earlier, using securities regulation is a global trend. At a similar time as the U.S. SEC started to regulate ICOs as securities in the DAO No Action Letter, many other countries started to consider ICO regulation. Because global regulation for cryptocurrency is not yet established, the Korean government has maintained the position that it will examine the regulatory process of other countries and global regulation to

---

[148] The author has argued that to regulate unfair trading at the cryptocurrency market, regulators should rely on FSCMA. Whayoon Song, *Legal Study of Unfair Trading on Virtual Asset Market*, 13.1 KOREAN J. BANKING & FIN. L. 346-50 (2020).

[149] *See Report from Study Group on Virtual Currency Exchange Services*, *supra* note 129, at 17.

[150] *See* Song, *supra* note 148, at 347-48.

[151] Youngwoo Shin, *supra* note 41, at 482-83.

[152] This amendment includes the introduction of virtual asset concept, several requirements for cryptocurrency exchanges such as certified information security management system. *See* Young Kim et al., *supra* note 40.

[153] *See* Song, *supra* note 148, at 347-48.

adopt regulatory regimes.[154] ICOs are conducted all around the world and investors can easily participate in other countries' ICOs online[155] so global regulatory cooperation will be important in the future.[156] In that matter, using the securities regulations regime as a model supports the Korean government's position.

Some people from the blockchain industry may oppose this position because financial regulation is too restrictive for the blockchain industry. However, as illustrated in Singapore, stronger regulation does not affect the promotion of ICOs. The expansion resulted from the influx of interested parties from other countries, attracted by the clear regulation and convenient infrastructure for the financial industry. Applying securities regulations to ICOs may attract foreign ICO firms which operate internationally and would prefer similar regulation everywhere.

B. Investment Contract Provision Will Not Be Feasible to Apply to Security Tokens

Regulators may consider recognizing securities tokens as securities, and therefore relying on investment contract provisions. However, considering the past cases and the Korean government's policy, it would not be feasible to use investment contract provisions when applying securities regulation to securities tokens in reality.

Investment contracts were introduced to the FSCMA to cover atypical financial products that do not fall into the typical securities definition.[157] This provision is developed from the investment contract

---

[154] *Cryptocurrency Task Force Meeting to Review the Actions of the Relevant Institutions*, *supra* note 8; *ICO Survey Results and Future Countermeasure*, *supra* note 30.

[155] Because of the global popularity of cryptocurrency, the International Organization of Securities Commissions ("IOSCO") has "identified crypto-assets as one of its top work priorities for 2019 and 2020." *See* IOSCO, *IOSCO Publishes Report on Education of Retail Investors Regarding Risks of Crypto-Assets*, (Dec. 22, 2020) https://www.iosco.org/news/pdf/IOSCONEWS587.pdf.

[156] For trading in secondary markets, IOSCO stated that global cooperation is important and IOSCO principles 13, 14, and 15 will apply. However, for ICO, there is no clear statement about global cooperation yet. INT'L ORG. OF SEC. COMM'NS, ISSUES, RISKS AND REGULATORY CONSIDERATIONS RELATING TO CRYPTO-ASSET TRADING PLATFORMS: FINAL REPORT, 26-27 (2020). Changmin Chun also pointed out that considering other countries have set up ICO regulations, it is time for Korean government to introduce a regulatory regime referring to global regulation. *See* Changmin Chun, *Overseas Virtual Asset Financing Regulation Status and Future Assignment, Presentation at 2019 Electronic Financing Seminar*, at 14, 50 (Dec. 18. 2019), http://www.bok.or.kr/portal/bbs/B0000232/view.do?nttId=10055437&menu No=200725.

[157] The FSCMA introduced "Financial Investment Instruments" which means 1) with an intention to gain profits or avoid loss; 2) a right acquired by an agreement to pay money or any other thing with property value at a specific point the present or in the future; 3) where there is a risk that the total amount of such money, etc., paid or payable, to acquire that right may exceed the total amount of money, etc. already recovered or recoverable from such right. Financial Investment Services and Capital Markets Act, Act No. 8635, Aug. 3, 2007, *amended*

concept, the *Howey* test for U.S. securities regulation of investment contracts.[158] FSCMA Article 4(6) defines "investment contract" as "1) instruments bearing the indication of a contractual right 2) under which a specific investor is entitled to the profits earned, or liable for losses sustained, 3) depending upon the results of a joint venture in which the specific investor invests money, etc. jointly with a third person and which is to be run mainly by the third person."[159] Issuers or third parties usually conduct ICO for a specific project, and investors expect to profit from their investments in said project. The DAO report concluded that ICOs are securities if they meet the *Howey* standard.[160] The Korean government may benchmark the regulatory mechanism developed by the U.S. SEC because it can rely on the investment contract provision of the FSCMA. However, unlike the U.S. SEC, Korea's FSC is reluctant to apply investment contract standards to specific cases.

In 2014, there were scams regarding sales of real estate in which third parties and investors agreed to pool real estate, rent units, and distribute the profits.[161] The FSC relied on Section 2 of the Fund Raising Act instead of investment contract securities of the FSCMA.[162] The FSC has not explained its holding, except to say that the investment contract securities can be used where the product does not have features of other preexisting securities types.[163] Jabonn Kim has analyzed why the FSC did not apply the investment contract approach to cryptocurrencies. He concludes that although the investment contract concept originated from U.S. securities regulations, the FSCMA definition of securities is based on "security types theory" unlike U.S. regulations.[164] So it is possible that under this theory the FSCMA would

---

by Act No. 11845, May 28, 2013, art. 3(1) (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/These Financial Investment Instruments are divided into securities and derivatives. The securities are classified into six categories: debt securities, equity securities, beneficiary securities, investment contract securities, derivative-linked securities, and depository securities. FSCMA, Act No. 8635, art. 4 (S. Kor.).

[158] 15 U.S.C. § 77b. The *Howey* test requires: 1) a person invests money, 2) in a common enterprise, 3) is led to expect profits, 4) solely from the efforts of another SEC v. Howey Co., 328 U.S. 293, 298 (1946).

[159] FSCMA, Act No. 8635, art. 3(1) (S. Kor.). The provisions of the FSCMA are similar to the *Howey* test. The expectation of profit prong is reflected in Section 3(1) of the FSCMA, the definition of Financial Investment Instrument. Unlike the fourth prong of the *Howey* test, the FSCMA clearly includes the cases in which investors participate in management of companies saying "mainly by third person" so clearly includes vertical commonality concept.

[160] The DAO, Exchange Act Release No. 81207, at 10-11 (July 25, 2017), https://www.sec.gov/ litigation/investreport/34-81207.pdf.

[161] Jinseong Lee, *Geum-yung-gamdog-won, Bulbeob 'Tujagyeyagjeung-gwon' Gyujee Yeojeonhi Sogeugjeog* [*Financial Supervisory Service Remains Passive Against Illegal 'Investment Contract Securities' Regulation*], Yoido Investors Rights Institute: Hannuri Law (June 20, 2014), http://yiri.co.kr/kr/?p=6109.

[162] *See id.*

[163] *See id.*

[164] Jabonn Kim, *Bitcoineun Jeungeouninga?* [*Is Bitcoin a Security?*], 19 JEUNGEOUNGBEOBHAKHEO [SEC. L. RES.] 171, 188, 192-93 (2018). He argued that the FSCMA classifies Financial Investment Instruments into securities and derivatives and then securities are divided into six kinds of securities while U.S. regulation provide broader definition.

not apply because cryptocurrency does not fall into the type of securities such as investment contracts.[165] Although the creators of the FSCMA intended to create flexible regulation, the FSCMA still keeps a limited definition. Importantly, he also points out the weakness of the FSC's enforcement power.[166]

I agree that the FSCMA defines securities as types in a clearer and more limited way than the U.S., resulting in the FSC having limited power. However, even if the FSC regulates cryptocurrency as investment contracts, problems remain because ICO firms must comply with duties of issuers such as filing registration statements, disclosure duties, and other requirements which are designed for listed companies and do not fit ICOs well. Also, each cryptocurrency has different characteristics and ICO firms and regulators should judge whether it is an investment contract. In this context, if regulators follow an investment contract approach, they should promulgate guidelines for judging and amending other rules. It would be very burdensome for the FSC to create guidelines by itself. The FSC may lack jurisdiction to apply the FSCMA to cryptocurrency, since cryptocurrencies have various characteristics and new products develop that can be cooperatively regulated by different departments such as IT related department. Thus, in these reasons, the investment contract approach is difficult to practically use.

Instead of relying on catch all provisions in an investment contract, Korean regulator can apply securities regulations reviewing features of tokens like the U.S. and Singaporean regulators do. However, it may make users confused and will be burdensome to regulator too. Therefore, Korean regulators should consider creating a new provision to include cryptocurrency as securities as Japanese regulators did and guidelines to distinguish between security type ICOs and non-security type ICOs.[167]

C. The Korean Government Should Limit ICO Participants to Protect Investors.

Because securities tokens have features of securities, ICO firms should comply with the FSCMA unless they are qualified for exemptions. However, the requirements of the FSCMA, such as filing registration statements and disclosing required information, are designed for listed companies and do not fit ICOs well. This incurs huge compliance cost for ICO firms and this leads ICO firms to seek exemptions. Also, the contents of the projects and the technology in ICOs are hard for the general public to understand. Therefore, the possibility of fraud is greater than in other transactions. Thus, to protect investors and the economy, it is better to limit market participants and the size of ICOs, especially in the beginning stage of

[165] *Id.* at 189-91, 193.
[166] *Id*. at 193, 197.
[167] *See* Song, *supra* note 148, at 350.

the market development. As ways to enjoy exemptions from the FSCMA, this research introduces crowdfunding laws and SAFT structure.

i. Crowdfunding Laws

The crowdfunding laws under the FSCMA support fundraising from investors by small to medium size firms.[168] The concept is similar to ICOs in that it is conducted online by startups targeting the general public, so it is possible to apply this law to the ICO regulations. In July 2015, the FSCMA was amended to introduce the crowdfunding brokerage business, and it became effective in January 2016.[169] Considering crowdfunding companies are usually small startups, the FSCMA designs regulations for crowdfunding brokers, not companies.[170] The FSCMA defines a crowdfunding broker as "an investment broker engaging in the online brokerage of public offering or sale of debt securities, equity securities and investment contract securities."[171] Once registered, an issuer can enjoy waiver from duties or lower duties of the FSCMA: Instead of submitting a registration statement, an issuer can upload information related to the financial status and condition of subject securities, among other possibilities.[172]

The crowdfunding law limited the issuers' annual issuance premium to around seven hundred million Korean won (around a hundred thousand dollars).[173] In order to strongly protect investors, the crowdfunding takes measures to set different investment amount limitations according to the level of knowledge on the financial market and the assets of investors.[174] The FSCMA classifies investors as either ordinary investors or professional investors.[175] The FSCMA defines professional investors as "investors who ha[ve] ability to take a risk accompanying investment."[176] Professional investors listed include the government, financial institutions, listed corporation, and others similarly situated and individuals whose assets including bank deposits, total more than 500 million won.[177] The FSCMA defines the ordinary investors as "investors other than professional

[168] FSCMA, Act No. 8635, art. 9(27) (S. Kor.).

[169] *See* Press Release, Financial Service Comm'n, Doib Doel Keulaudeu Peonding [Crowdfunding to be Introduced] (July 23, 2015). The author takes sole responsibility for this source.

[170] HYE HWAL SEONG, CAPITAL MARKET ACT, 235 (Capital Books, 2018).

[171] FSCMA, Act No. 8635, art. 9(27) (S. Kor.).

[172] *Id*.

[173] *See* Press Release, Financial Service Comm'n, *supra* note 168.

[174] FSCMA, Act No. 8635, art. 117-10(6) (S. Kor.); SEONG, *supra* note 170, at 236.

[175] FSCMA, Act No. 8635, art. 9(5)-(6) (S. Kor.).

[176] FSCMA, Act No. 8635, art. 9(5) (S. Kor.).

[177] Enforcement Decree of FSCMA, Presidential Decree No. 28796, April 10, 2018, art. 10 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr/ (last visited May 20, 2021).

investors."[178] The crowdfunding law limits the amount of investment allowed according to income. However, for professional investors, there is no limit.[179]

Because funding by ICOs is conducted online by startups and many individual investors, its concept is similar to crowdfunding brokerage. So, it is cost effective to use this regulatory mechanism. The regulator can use some concepts of this regulation such as limitations of participants and ICOs amount.

The concept of the current crowdfunding laws could be used or amended for the ICOs regulation. Brokerage firms can play a role as a gatekeeper to protect investors. As licensed third parties, the brokerage firms should be given the responsibility to review the financial conditions, and the project progress of the ICOs. Second, current crowdfunding law classifies investors into three types and allows ordinary investors to participate in ICOs.[180] Considering that the disclosure requirements for ICOs are insufficient to adequately protect investors, it is easy to understand why fraud is prevalent. Therefore, it is better to limit the market to professional investors. Limits on the amount invested in ICOs should be increased to at least twice the current limit. The average ICO amount last year in the Korean ICO firms were 30 billion won,[181] but the limitation on total issuance amount in crowdfunding is only 1.5 billion won.[182] Third, conditions for traditional securities such as one-year resale restrictions, one-year lock-up limitation for issuers, and controlling shareholder are not applicable to ICOs, so it should be repealed for ICO regulations.

In short, crowdfunding laws in the FSCMA can be used for ICOs. ICO firms take advantage of the eased disclosure requirements and the limited investors of ICOs.

ii. Utilizing Simple Agreements for Future Tokens

ICO firms also may limit the scope of ICO to the institutional investors by entering SAFTs between ICO firms and institutional investors, especially in the beginning stage of the market development as U.S. ICOs firms utilize. Although SAFT is designed to sales to institutional investors, this should not be used to avoid disclosure requirements of securities

---

[178] Enforcement Decree of FSCMA, art. 10(17) (S. Kor.). It sets the requirement following and the designation as professional investors is assigned.

[179] *See* Press Release, Financial Service Comm'n, *supra* note 169.

[180] FSCMA, Act No. 8635, art. 117-10(6) (S. Kor.); SEONG, *supra* note 170, at 236.

[181] *ICO Survey Results and Future Countermeasures, supra* note 30.

[182] FSCMA, Act No. 8635, art. 117-10 (S. Kor.); *see* FSCMA, Act No. 8635, Enforcement Decree of FSCMA, art. 117-15(1) (S. Kor.). The limitation on total issuance amount in crowdfunding used to be 0.7 billion, but the government increased to 1.5 billion to support the stable fundraising. Press Release, Financial Service Comm'n, FSC Proposes Capital Market Reform (Nov. 1, 2018), https://www.fsc.go.kr/eng/pr010101/22193.

regulations, as expressed by the U.S. court,[183] which may potentially make the market exceptionally limited.

D. The Korean Government Should Strengthen Disclosures of Utility Tokens

The purpose of utility tokens is to provide tokens for the exchange of services and items for consumption.[184] In this manner, it is not a security, nor is it the object of securities regulation. However, many times the ICO firms rely on the utility token appearance to avoid regulation. Many investors also purchase utility tokens in expectation of profits, not only means of exchange with services and products. This situation makes regulations ambiguous and creates a loophole. It is better to make a two-tiered framework which (i) includes utility tokens with securities features; and (ii) is a system for pure utility tokens.

First, for pure utility tokens, appropriate disclosure is important and regulators should have information about ICOs in case the ICOs are illegal. In this context, the new regulatory regime in France is worth discussing. In 2019, the French government introduced the new regulations for utility tokens which states that ICO firms can ask for the approval of the French Financial Market Authority ("AMF").[185] Approval by the AMF, known as an AMF visa, is optional and the AMF will disclose the entities to receive AMF visas on the AMF's website.[186] Because this visa from the AMF will be granted if ICO firms meet with certain requirements such as adequate disclosures,[187] investors may be more relieved about the status of the ICOs. Instead of requesting approval, ICO firms can submit disclosure documents to AMF to help investors make informed decisions.[188]

---

[183] *See, e.g.*, SEC v. Telegram Grp. Inc., 448 F. Supp. 3d 352 (S.D.N.Y. 2020).

[184] *See* William Hinman, *supra* note 74.

[185] In 2018, "The Plan d'Action pour la Croissance et la Transformation des Entreprises (PACTE – Action Plan for Business Growth and Transformation)" was proposed and it was enacted in 2019. The French government said that the purpose is "eliminating barriers to business growth at every stage of business development, from business transfers, including financing" to companies with innovations (Bruno Le Maire, Minister of Economy and Finance, and Delphine Geny-Stephann, Minister of State, attached to the Minister of Economy and Finance). This bill suggests the new regulatory regime to ICOs, enforcement measures about non-compliance with the foreign investments rules. *PACTE, the Action Plan for Business Growth and Transformation*, GOUVERNEMENT.FR, https://www.gouvernement.fr/en/pacte-the-action-plan-for-business-growth-and-transformation (last visited May 21, 2021).

[186] *See* PARIS EUROPLACE, FRANCE'S NEW FRAMEWORK FOR ICOS AND TOKENS: SIMPLE, ATTRACTIVE AND PROTECTIVE 4 (Apr. 2019), https://www.paris-europlace.com/sites/default/files/public/pariseuroplace_brochure_francesnewframeworkforicos andtokens_april_2019-compresse.pdf; *see also* Clifford Chance, *France Leads the Way with a Dedicated Legal Regime for Digital Assets and ICOs*, CLIFFORD CHANCE (Nov. 2019), https://www.cliffordchance.com/content/dam/cliffordchance/briefings/2019/07/france-leads-the-way-with-a-dedicated-legal-regime-for-digital-assets-and-icos.pdf.

[187] *See* PARIS EUROPLACE, *supra* note 186.

[188] *Id.* at 3.

There is an argument for another agency, such as the Consumer Protection Agency, to be responsible for the registration or approval. However, for efficient regulation, it is better to have one regulatory organization govern both ICOs and cryptocurrency trading. That way regulators also can be aware of ICO and cryptocurrency status and take action when it is necessary. Also, issuers' compliance cost will be lower. Currently, in the U.S. issuers must research and comply with regulations from several organizations including FinCen, the SEC, and the CFTC.[189] Additionally, different states develop different regulations.[190] These are heavy compliance burdens for issuers. The Korean government should delegate power to one organization such as the FSC or establish a new organization that cooperates with the relevant entities.

Second, when the regulator finds that a utility token has any features of a security, the regulator should recommend that such issuers follow the regulation for security tokens. Considering compliance cost and vulnerability of investors, regulators may recommend utilization of crowdfunding laws or SAFT in such cases. In short, for the pure utility tokens, adequate disclosure process should be adopted referring to the AMF's visa. For the utility token with security features, regulators need to recommend following regulation for security tokens to protect investors.

E. For Investor Protection, ICO Firms Should be Required to Disclose Enough Information Appropriately

Many investors in Korea, often older adults, do not know much about cryptocurrencies, yet they have invested their money in ICOs or cryptocurrency trading and have suffered losses because of fraud.[191] Therefore, it is essential to think about protecting cryptocurrency investors. The first problem in the ICO market is information asymmetry between issuers and investors. Compared to issuers required to disclose continuous information about an IPO, cryptocurrency issuers disclose minimal information. They provide information through their website and white papers, where issuers explain the project plan and structure.[192] Moreover,

---

[189] Michael Losavio, Mark Wettle & Adrian Lauf, *Cryptocurrency: Regulating Poetry*, 83(5) BENCH & B. 14, 16 (2018).

[190] *See id*.

[191] *See* Adam James, *Older South Koreans Are the Biggest Investors in Cryptocurrencies*, BITCOINIST, https://bitcoinist.com/older-south-korea-invest-bitcoin-crypto/ (last visited May 21, 2021). Cryptocurrency related frauds that FSA referred to prosecutor's office is rapidly increasing. *Geomchal, gasanghwapae sagi jipjung danseoknaseobda [Prosecutor Begins Intense Investigation on Cryptocurrency Related Fraud]*, THE HANKYOREH (Feb. 21, 2018), http://www.hani.co.kr/arti/society/society general/833019.html ("[T]he number of pseudo-receiving crimes related to cryptocurrency commissioned by the Financial Supervisory Service to the police is steadily increasing from 12 in 2015 to 23 in 2016 and 38 in 2017.").

[192] Dell Eraba, *supra* note 2, at 1112.

white papers usually do not provide specific information about issuers.[193] Around 55% of white papers did not provide issuer's contact information accurately.[194] Also, around 82% of white papers did not provide the regulatory status of ICOs,[195] around 25% of white papers do not offer information about financial status,[196] and more than 96% do not provide information about segregation of funds.[197]

Thus, regulators should provide the framework for the information that issuer should provide in the white paper, such as by way of a standard form, and verify that information. If the information is incorrect, regulators should not approve the ICO. The information should include the issuer's personal information such as name, address and contact. Also, it should include the financial status of issuer and the project, the plan to use funds from the ICO, and the features of the cryptocurrency.[198] To make comparisons easier, a regulator should provide a template for disclosure. After the ICO, issuers should also disclose information about what its financial status is, how the project is developing, and how the funds were used. For effective regulation, the government may delegate self-regulatory organization to rate the quality of ICOs. It is similar to the rating funds or evaluating the quality disclosure of listed companies and disclosing each penalty points of the listed companies to the public via the Korea Exchange.[199]

F. Regulation Should Be Flexible to Reflect Rapid Development of Industry

As the cryptocurrency industry is rapidly developing, regulation should be flexible enough to adapt these changes. Self-regulation and a regulatory sandbox may contribute to flexibility from insights of global regulation research.

---

[193] Zetsche et al., *supra* note 5, at 11.

[194] *Id*. at 16.

[195] *Id*. at 11.

[196] *Id*. at 15.

[197] *Id*.

[198] *Id*. at 39; *see generally* Hye Hwal Seong, *Gasanghwapae gongmowa sangjange daehan jeokjeonggyujaebangan* [*A Study on the Optimal Regulation on Initial Coin Offering (ICO) and the Listing of Cryptocurrency*], 37 SANGSABEOBYEONGU [COM. L. RES.] 63 (2018).

[199] Korea Exchange levy the penalty score to listed companies not complying disclosure rules and when the penalty scores reach to the certain level, such companies may be delisted. KOSPI Market Disclosure Regulation, Jan. 21, 2005, *amended on* July 22, 2015, art. 35 (S. Kor.), *translated in* Korea Exchange homepage, http://global.krx.co.kr/ (last visited May 21, 2021); Enforcement Rules of KOSPI Market Listing Regulation, Jan. 27, 2005, *amended on* May 13, 2013, art. 13 (S. Kor.), *translated in* Korea Exchange homepage, http://global.krx.co.kr/ (last visited May 21, 2021).

i. ICO Self-Regulation

While there is no clear regulation by the government, it is worthwhile experimenting with self-regulation.[200] Self-regulation will play a role as the gap-filler when government regulation does not exist.[201] Also because the Korean government worries about the effects of new regulation on cryptocurrency, regulators may use the self-regulation for 'testing the water' before introducing the governmental regulation.[202] Currently, KCBA's self-regulation framework proposes cryptocurrency exchanges use KCBA's listing guideline but a detailed guideline is not yet available to the public.[203] Considering that considerable fraud occurs in ICO stage, it is better to structure more detailed regulation on ICOs. In structuring the framework, cooperation with the Korean government would be essential. So, the Korean government should react more actively on cryptocurrency regulation. Moreover, appropriate enforcement of self-regulation is as important as well-structured regulation. As the government regularly audits self-regulatory organization in the securities market and approve the rules of self-regulation under the FSCMA,[204] the Korean government should involve itself more proactively in the beginning stage of self-regulation.

Among self-regulatory organizations, exchanges can play a gatekeeper role in ICOs regulation because they are the entities that have power of approval of listing/delisting and have custody of the cash. Hye Hwal Seong argues that exchanges should disclose the listing and delisting policy, and the regulator may suggest the standard form of listing standard.[205] His reasoning is based on comparing exchange regulations containing a clear listing/delisting standard and disclosure policy with exchanges that do not.[206] In April 2018, a few exchanges disclosed a listing or delisting policy.[207] Only one exchange had a listing standard and asked issuer for detailed disclosure. Almost three year later, in April 2021, more exchanges disclose their listing or delisting policy compared to the situation in April 2018.[208] Although there

[200] The author also proposes self-regulation in secondary markets of cryptocurrency to effectively regulate unfair behaviors such as price manipulation. Song, *supra* note 148, at 353-354; *see also* Whayoon Song, *Legal Study to activate Self-Regulation for Unfair Behavior of Virtual Asset Market*, 22 (1) KOREAN SEC. L.J. 183, (2021).

[201] *See* Joon-Young Kim & Hyung-Seok Han, *supra* note 32.

[202] *See id.*

[203] In October 2018, KBCA proposed ICO and exchange guideline at a discussion session, the Blockchain ABC Korea where senators, governmental officers, etc., participated but this guideline is not in public. Press Release, Korean Blockchain Association, Proposed ICO and Exchange Guideline (October 4, 2018), https://www.kblockchain.org/board/press/read/621?nPage=4.

[204] FSCMA, Act No. 8635, art. 283 (S. Kor.).

[205] Seong, *supra* note 198, at 89-91.

[206] *Id*.

[207] *Id.* at 73-74.

[208] Currently, all four exchanges (Bithumb, Coinone, Upbit, Korbit) have listing standard, checklist or guideline. Jeong In-sun, *[Opening the Exchange] ④ Coin Listing,*

was no regulation, exchanges started to disclose listing or delisting standards, even though those standards seem to be vague and arbitrary.[209] As mentioned above, exchanges play an important part in regulating ICOs. If exchanges arbitrarily list and delist or otherwise act arbitrarily, transparency and fairness in the market will decline. Thus, regulators need to propose principles for a listing standard which guides exchanges without sacrificing their self-regulatory work.

ii. Application of a Regulatory Sandbox to ICO

As Singapore launched its Regulatory Sandbox benchmarked on the British model,[210] the Korean government also started its Regulatory Sandbox to encourage companies to test innovative services and products in the real world. On April 1, 2019, the Special Law on Supporting Financial Revolution became effective and introduced the Regulatory Sandbox in financial services.[211] Under this Regulatory Sandbox in financial services, financial institutions or corporations can test the new products or services when it is not clear whether they are legal.[212] Once the Innovative Financial products and Services Review Committee of the FSC receives applications, it reviews them using eight criteria including innovation.[213] Once approved, the applicant is exempt from the thirty four financial laws including the FSCMA.[214] In 2019, ICO firms have not applied for this review because of the policy banning ICOs. [215] Moreover, the few ICO firms that have applied have been rejected.[216]

The Korean government can utilize this Fintech Sandbox for ICO as the Singapore Government does. However, the Korean government has maintained that ICOs are speculative.[217] To take advantage of the Fintech Sandbox in regulating ICOs, the Korean government's stance needs to

---

Upbit>Coinone>Bbitsum>Kobit, COINDESK KOREA (Mar. 10, 2021), http://www.coindeskkorea.com/news/articleView.html?idxno=72976.

[209] SEONG, *supra* note 170, at 73.

[210] PARK HYUN-OK, ISSUE REPORT 2019-10: THE ENGINE OF INNOVATION IN MAJOR COUNTRIES, REGULATORY SANDBOX 6 (NIPA, 2019).

[211] Geumwunghyeoksinjiweonteukbeolbeob [Special Act on Support For Financial Innovation] Act No. 16183, December 31, 2018 (S. Kor.), *translated in* Korea Legislation Research Institute online database, https://elaw.klri.re.kr. This law was created and announced December 2018 and became effective April 2019. SANDBOX KOREA, OVERVIEW, https://sandbox.fintech.or.kr/financial/overview.do?lang=en (last visited May 21, 2021).

[212] *Id.*

[213] SANDBOX KOREA, INTRODUCTION, https://sandbox.fintech.or.kr/financial/financial_introduction.do?lang=en (last visited May 21, 2021).

[214] *Id*.

[215] *See also* Press Release, Financial Service Comm'n, FSC Gyuje saendeu bagseuui 'hyeogsin geum-yung seobiseu'lo jijeongdoen du beonjjae geum-yung seobiseu jegong eobche [Second Batch of Financial Service Providers Designated as 'Innovative Financial Services' for FSC's Regulatory Sandbox] (May 2, 2019), https://www.fsc.go.kr/eng/pr010101/22211.

[216] *See also id.*

[217] *ICO Survey Results and Future Countermeasures*, *supra* note 30.

change in order to save social cost for legislation, administration and eventually promote blockchain industry.

VI. CONCLUSION

The blockchain is one of the core technical infrastructures of the fourth industrial revolution. ICOs are the fundraising tool that enable the blockchain industry to develop. The Korean government has a policy to support the development of the blockchain industry and to lead technological innovation in the world. However, the policy banning ICOs hinders the development of the blockchain industry. To promote its growth, the government should not ban ICOs because they contain speculative features. Instead, the government should regulate ICOs to protect investors.

The Korean government can rely on the framework for regulating the securities market in the FSCMA because there is the same need to protect investors and promote transparency. Moreover, this would follow the global trend. Since the U.S. SEC has applied the *Howey* test to ICOs, most countries have started to rely on a securities regulation model. However, the U.S. regulatory regime is not the best fit for every country. The *Howey* test is very flexible and convenient, but it can suppress ICOs more than necessary. The Korean government should consider the most appropriate method to regulate ICOs in Korea. Specifically, to protect investors, the government can limit the market to sophisticated investors or limit the ICO size. The government could also require that sufficient information be disclosed to potential investors in utility tokens to allow them to make an intelligent investment decision.

People compare the sharp increase and decrease of cryptocurrency's price to the dot-com bubble in the early 2000s.[218] The price of cryptocurrency will probably go up and down for a while. However, just as the dot-com period becomes the inflection point in the creation of a flourishing economy based on the internet, the ICO bubble is also expected to be the foundation of another economic success based on blockchain industry. Considering the current demand for ICOs in Korea and the expected development of the blockchain industry, continuing the policy of banning ICOs cannot be the right solution. It is time to introduce new regulations on ICOs and take an important step toward the future of the blockchain industry.

[218] *See* Cole Peterson, *Crypto Price Crash Similar to the Dot-Com Bubble, and That's not a Bad Thing*, NEWSBTC (Sept. 12, 2018), https://www.newsbtc.com/2018/09/12/crypto-price-crash-similar-to-dot-com-bubble-and-thats-not-a-bad-thing.

THE NEW "ARMS" RACE: HOW THE U.S. AND CHINA ARE USING GOVERNMENT AUTHORITIES IN THE RACE TO CONTROL 5G WEARABLE TECHNOLOGY

*Kirsten S. Lowell**

I. INTRODUCTION

Imagine waking up and putting in your contact lenses. For many, this is an everyday occurrence, but these contacts are different. These contacts are a new form of wearable technology.[1] You can see clearly, and you can also read what emails you received overnight, your to-do list for the day – without ever having to look down at a phone or computer. The contact lenses are your assistant – they see everything you do and can provide suggestions and directions in real time.[2] This scenario is coming soon with 5G wearable technology.[3] Along with this technological evolution comes a host of new national security issues. While the broad introduction of wearable 5G technologies may revolutionize daily life, the amount of personal data they collect is immense, and the potential for national security risks is even more significant. China and other foreign countries could collect everything you see.

Wearable technology offers convenient real-time location services, health data, video, continuous recording, and listening.[4] Wearable technology also presents national security and privacy concerns because companies, hackers, and governments can use personal data and data aggregated across users for nefarious purposes.

Wearable technology especially is fueled by 5G technology, the latest innovation in mobile broadband technology. 5G technology is more than 1000% faster than the current system.[5] The benefits of 5G technology

* George Mason University, Antonin Scalia Law School, J.D. graduated May 2021. I would like to thank Michael and Jocelyn Lowell and Michael Beville for their encouragement and guidance throughout this process. I am also thankful to the George Mason International Law Journal editors and members for their thoughtful comments and edits.

[1] *See* Martin Gee et. al., *A Day in the Life of Wearable Technology*, TIME, https://time.com/see-the-wearable-tech-of-the-future/ (last visited Apr. 16, 2021). Smart contact lenses are in the research and development phase but will likely be sold in markets in a few years. *See* Julian Chokkattu, *The Display of the Future Might Be in Your Contact Lens*, WIRED (Jan. 16, 2020), https://www.wired.com/story/mojo-vision-smart-contact-lens/; MOJO VISION, https://www.mojo.vision (last visited Apr. 16, 2021).

[2] *See* Chokkattu, *supra* note 1.

[3] *See* Jennifer Alsever, *With 5G, Wearable Devices are Expected to Become Even More Sci-Fi,* FORTUNE (Mar. 24, 2020), https://fortune.com/2020/03/24/5g-wearable-devices/.

[4] *See* JILL C. GALLAGHER & MICHAEL DEVINE, CONG. RSCH. SERV., R45485, FIFTH-GENERATION (5G) TELECOMMUNICATIONS TECHNOLOGIES: ISSUES FOR CONGRESS, 6 (2019).

[5] *See id.*

are vast as system speed is a precursor to innovation.[6] The increase in speed will be felt throughout the world, impacting every part of our lives and our economy.[7] Innovations driven by 5G technology may drive new opportunities for work, higher GDP, and foster even more significant innovation. Consequently, the United States and the People's Republic of China are racing to lead on 5G technology to capitalize on the economic and innovative opportunities it brings.

The country where domestic 5G is successfully implemented first will likely win the global race.[8] Companies headquartered or located in that country will be able to deploy and potentially control communications networks and infrastructure across major economies around the world,[9] and that country's government will establish the standards for 5G.[10] Setting the standards gives the government an edge in both regulating and controlling the technology.[11] A dominant presence in the market and the first opportunity to establish standards used in practice may create opportunities for the government to monitor, regulate, prevent, manipulate, or interfere with communications.[12] The government could locate wearable technology users and access the data on the user's device[13] or collect personal information like the user's heartbeat or what the user can hear and see (including sounds and sights not visible or audible to the human being).[14]

---

[6] *See* Michael Ringel et al., *The Rising Need for Innovation Speed*, BCG (Dec. 2, 2015), https://www.bcg.com/publications/2015/growth-lean-manufacturing-rising-need-for-innovation-speed.

[7] *See id.* at 3. The military's intelligence, surveillance, and reconnaissance systems and processing, command and control, and logistics systems may be improved significantly by using 5G. *See* JOHN R. HOEHN & KELLEY M. SAYLER, CONG. RSCH. SERV., IF11251, NATIONAL SECURITY IMPLICATIONS OF FIFTH GENERATION (5G) MOBILE TECHNOLOGIES (2021), https://fas.org/sgp/crs/natsec/IF11251.pdf.

[8] Marguerite Reardon, *5G Will Change the World. China Wants to Lead the Way*, CNET (July 10, 2020), https://www.cnet.com/news/5g-will-change-the-world-and-china-wants-to-lead-the-way/. China will likely deploy the first 5G wide-area network; however, Chinese technologies mainly rely on sub-6 (mid band and low band spectrum *discussed below)* technologies and have had failures in their domestic plan to roll out 5G. *See id.* China has faced a severe global backlash from the U.S., India, and the U.K., leading those countries to "rip and replace" Chinese Huawei technology. *See id.* Accordingly, the race is far from won.

[9] *See id.*

[10] *See* GALLAGHER & DEVINE, *supra* note 4, at 13-14.

[11] *See id.*

[12] *See* Adam D. Thierer, *The Internet of Things and Wearable Technology: Addressing Privacy and Security Concerns without Derailing Innovation*, 21 RICH. J.L. & TECH. 6, 40-44 (2015); Jim Baker, *Counterintelligence Implications of Artificial Intelligence – Part III*, LAWFARE BLOG (Oct. 10, 2018), https://www.lawfareblog.com/counterintelligence-implications-artificial-intelligence-part-iii.

[13] *See id.*

[14] *See id.* Wearable technology can hear more than the human ear and see further than the human eyes. *"Smart Eye," A Computer Inside Our Eyes*, SK HYNIX NEWSROOM (Apr. 29, 2020), https://news.skhynix.com/smart-eye-a-computer-inside-our-eyes/ (superior to human eyes); American Friends of Tel Aviv University, *New Technology Allows Cameras to Capture Colors Invisible to the Human Eye*, SCIENCEDAILY (Nov. 5, 2020), https://www.sciencedaily.com/releases/2020/11/201105113027.htm; Ariel Schwartz, *Boost*

The U.S. and China are competing to develop the first domestic employment of 5G technology.[15] Both countries use government support to boost their own industries' development of 5G technology and interfere with or interrupt development in the other country.[16] However, the governments have taken different approaches to incentivize 5G development. China's political system enables a government-directed focus on 5G.[17] In contrast, the U.S. relies on the private sector with governmental support.[18]

China's government-directed focus is mainly implemented through its nationwide plan to be the leader in 5G technology.[19] The Chinese government supports the 5G industry by implementing regulations on imports and foreign investments to limit domestic competition; subsidizing research, development, manufacturing, and procurement of materials and supplies; and leveraging military and intelligence assets to support industrial espionage.[20]

On the other hand, the U.S. political system relies largely on market forces for competition and innovation.[21] This primary reliance on market forces means that unlike China, the U.S. does not have a national plan to develop a 5G system. Instead, private companies compete against each other to create their own networks.[22] While recognizing the natural advantages of a market-based economy, which if left to their own devices would be expected to yield better innovation and technology, a successful effort in the U.S. will require additional legal authorities to prevent or mitigate Chinese interference.

With the growth of wearable technology fueled by 5G infrastructure, concerns arise with the increasing risk from foreign investors gaining access to increasing amount of U.S. citizens' personal data. Foreign investment in critical technologies, including those that will support innovation in the 5G development, and especially Chinese investment in those technologies,

---

Your Ears to Superhuman Levels With These Cyborg Ears, FAST CO. (Jun. 24, 2014), https://www.fastcompany.com/3032226/boost-your-ears-to-superhuman-levels-with-these-hearing-aids-for-people-who-can-h. Both sound and sight can be recorded and analyzed, causing even more access to data than ever before. *See generally* Ke Wan Ching & Manmeet Mahinderjit Singh, *Wearable Technology Devices Security and Privacy Vulnerability Analysis*, 8 INT'L J. NETWORK SEC. & ITS APPLICATIONS 19 (May 2016).

[15] Nicol Turner Lee, *Navigating the U.S.-China 5G Competition*, BROOKINGS INST. (Apr. 2020), https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_5g_competition_turner_lee_v2.pdf.

[16] *See id.*; INSA Cyber Council, *The National Security Challenges of Fifth Generation (5G) Wireless Communications*, INTEL. & NAT'L SEC. ALL., 4 (June 2019), https://www.insaonline.org/wp-content/uploads/2019/06/INSA_WP_5G_v5_Pgs.pdf.

[17] *See* GALLAGHER & DEVINE, *supra* note 4, at 13-14.

[18] *See id.*

[19] *See id.*

[20] *See id.*

[21] *See id.*

[22] *See id.*

creates critical risks that the U.S. is trying to mitigate.[23] One major effort to mitigate those risks is through the foreign direct investment review process at the Committee on Foreign Investment in the United States (CFIUS).[24] CFIUS is an interagency committee that reviews foreign investments in the U.S. with responsibility to make recommendations to the President to block transactions that threaten U.S. national security.[25]

In 2018, Congress expanded CFIUS's jurisdiction to better protect U.S. businesses from nefarious foreign investments.[26] By passing the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA), Congress amended CFIUS's existing statutory authority and provided new requirements for mandatory reviews and additional tools to protect national security in foreign investments.[27]

However, to the extent Congress intended CFIUS to help implement a strategy to win the race to dominate 5G through safeguarding U.S. technology, lawmakers need to recognize and address the inherent weaknesses in the export control system upon which CFIUS mandatory filing requirements are in part based. The export controls regulatory scheme is primarily reliant on individual companies reviewing regulations that are often vague or ambiguous and correctly making determinations about the laws that apply to their technology, a process often called "self-classification." While there are mechanisms by which the government may itself determine the laws that apply to a given technology pursuant to existing statutory and regulatory authorities, in practice, the uncertain self-classification process is the primary foundation of FIRRMA's "critical technologies" prong for mandatory CFIUS review procedures.

While Congress rightly updated and expanded CFIUS legal authorities, the "critical technology" definition for mandatory filing is based on an export controls system that mainly depends on companies' self-determinations. The regulations are complex, prone to uncertainty in some areas, and may be applied differently by different parties.

This comment suggests that Congress improve clarity and strengthen the CFIUS process by requiring more mandatory filings from

---

[23] Council on Foreign Relations, *Chinese Investment in Critical U.S. Technology: Risks to U.S. Security Interests* (Oct. 16, 2017), https://www.cfr.org/report/chinese-investment-critical-us-technology-risks-us-security-interests. FBI Director Christopher Wray says, "the greatest long-term threat to our nation's information and intellectual property, and to our economic vitality, is the counterintelligence and economic espionage threat from China." FBI, *The China Threat*, https://www.fbi.gov/investigate/counterintelligence/the-china-threat (last visited Apr. 16, 2021).

[24] *See generally* JAMES K. JACKSON, CONG. RSCH. SERV., RL33388, THE COMMITTEE ON FOREIGN INVESTMENT IN THE UNITED STATES (2020).

[25] *See* Amy Deen Westbrook, *Securing the Nation or Entrenching the Board? The Evolution of CFIUS Review of Corporate Acquisitions*, 102 MARQ. L. REV. 643 (2019); 31 C.F.R. § 800.101 (2020).

[26] *See* 31 C.F.R. § 800.101 (2020).

[27] *See id.*

countries of specific concern, strengthen the "critical technologies" provisions under FIRRMA by removing a reliance on export controls systems, and requiring mandatory disclosures to identify businesses of concern. Similarly, this comment argues that Congress should allocate more resources to improve processing times, release more details to the public about determinations made, and proactively engage with 5G industry participants (particularly small and mid-size companies) to ensure they are able to identify critical technologies.

Part II will discuss the background of 5G wearable technology, including the past technologies and current U.S. and Chinese law. Part III will analyze the CFIUS-FIRRMA scheme's problems regarding 5G wearable technology and will provide a solution. Finally, Part IV will conclude that the solution allows the U.S. to become the leader in the 5G Race while looking towards the future and its relations with China.

II. BACKGROUND

To understand the importance of CFIUS's involvement in 5G wearable technology, first, this section will explain 5G technology and wearable technology. Second, it will discuss CFIUS and other relevant U.S. laws. Third, this section will discuss the Chinese threat to data privacy and national security.

A. 5G Wearable Technology

5G Technology provides "faster speeds, greater capacity, and potential to support new features and services."[28] 5G technology is measured in megabits per second (Mbps). Mbps is the speed at which information is downloaded from or uploaded to the internet. 5G provides 1000-1400 Mbps or 3-4 seconds to download a 2-hour movie.[29] In contrast, 4G used 10-100 Mbps or 6 minutes to download a 2-hour movie.[30] Two major organizations develop the 5G Standard: the 3rd Generation Partnership Project and the United Nations International Telecommunications Union.[31] Once they approve a standard, industries around the world utilize the new uniform standard.[32]

The U.S. uses a market-based approach to 5G development. On October 1, 2018, "Verizon launched fixed 5G services in four cities."[33] As of February 2021, Verizon's 5G network is available in around sixty cities, with

[28] GALLAGHER & DEVINE, *supra* note 4, at 2.
[29] *See id.*
[30] *See id.*
[31] *See id.* at 12.
[32] *See id.*
[33] *See id.* at 10.

5G Home Internet available in eighteen select areas.[34] AT&T launched mobile 5G in twelve cities on December 21, 2018, with nineteen more targeted in 2019.[35] As of February 2021, AT&T reaches about 500 areas with 5G using low-band spectrum, and parts of thirty-eight cities with 5G+ using millimeter wave spectrum which is even faster. [36] T-Mobile officially launched its nationwide 5G network on December 2, 2019, but only to limited areas and for limited phones capable of accessing 5G.[37] Sprint planned to deploy 5G in 9 cities in the first half of 2019.[38] Sprint and T-Mobile merged and now have coverage to over 80% of Americans.[39] 5G serves current consumer demands and future applications globally. Current networks cannot keep up with demands for data.[40] As 5G is being implemented in the U.S., providers have faced problems with installing the appropriate hardware causing slow speeds, unstable connections, delays, or loss of service.[41]

5G creates significant consumer, industrial, and economic benefits. 5G benefits consumers because they can connect to the Internet of Things, making life convenient. The Internet of Things is "the collection of physical objects that interconnect to form networks of devices and systems that can collect and compute data from many sources."[42] Industries rely on the Internet of Things for their business operations.[43] The economic benefits are vast. In the U.S., 5G is expected to create three million new jobs[44] and provide $500 billion to the U.S. GDP.[45] Globally, 5G is expected to create $12.3 trillion in sales activities across multiple industries[46] and provide twenty-two million jobs by 2035.[47]

The following sections will explain 5G technology, wearable technology and the Internet of Things, and the Race to 5G.

---

[34] *See What Is 5G?,* VERIZON, https://www.verizon.com/about/our-company/5g/what-5g (last visited Apr. 16, 2021); *Verizon 5G Home FAQs- Ultra-fast Home Internet,* VERIZON, https://www.verizon.com/support/5g-home-faqs/ (last visited Apr. 16, 2021).

[35] GALLAGHER & DEVINE, *supra* note 4, at 10.

[36] *AT&T Rolls Out Super-Fast 5G+ Across the U.S.*, AT&T (Feb. 1, 2021), https://about.att.com/newsroom/2021/5g_plus.html.

[37] GALLAGHER & DEVINE, *supra* note 4, at 10.

[38] *See id.*

[39] *Coverage Check*, T-MOBILE USA, https://www.t-mobile.com/coverage/coverage-map (last visited Apr. 16, 2021).

[40] GALLAGHER & DEVINE, *supra* note 4, at 5.

[41] *See id.*

[42] *See id.*

[43] *See id.* at 1.

[44] *See id.* at 7.

[45] *See id.*; *see also* Accenture Strategy, *Smart Cities: How 5G Can Help Municipalities Become Vibrant Smart Cities* (Jan. 12, 2017), https://newsroom.accenture.com/content/1101/files/Accenture_5G-Municipalities-Become-Smart-Cities.pdf.

[46] *See* GALLAGHER & DEVINE, *supra* note 4, at 7; *see also* David Abecassis, *Global Race to 5G—Spectrum and Infrastructure Plans and Priorities*, ANALYSYS MASON, 7 (Apr. 2018), https://api.ctia.org/wp-content/uploads/2018/04/Analysys-Mason-Global-Race-To-5G_2018.pdf.

[47] *See* GALLAGHER & DEVINE, *supra* note 4, at 7.

i. A Brief Introduction to How 5G Technology Works

5G technology is made possible using millimeter waves. Millimeter waves on the spectrum provide greater bandwidth and speed. However, the millimeter waves cannot travel long distances or penetrate obstacles, so small cell sites are placed closer together to relay signals around the obstacles.[48] Small cells are "low-powered, short-range, low-cost, self-contained cell site nodes..."[49] They can be installed on poles, billboards, sides of buildings.[50] More than 800,000 small cells need to be installed by 2026.[51] In the future, it will be hard to go anywhere without seeing a small cell. They will be installed all over the country in every urban, suburban, and rural area to expand 5G connectivity. Additionally, more satellites will be launched to work with 5G networks, including mega-constellations like Starlink, to provide 5G in hard-to-reach places.[52]

Spectrum is the "radio frequencies used to communicate over airwaves."[53] Different "segments of spectrum are allocated to different uses," like mobile communications and broadcasting.[54] 5G technology uses three main segments of spectrum: high band (a.k.a. millimeter wave); mid band; and low band.[55] Mid band and low band are referred to as "sub-6."[56] Companies and other users may purchase rights at auctions or are assigned frequencies.[57] Companies use "infrastructure (e.g., towers, equipment) that enable[s] communications on their assigned frequencies."[58] Different federal agencies support broadcasting. The Federal Communications Commission (FCC) "manage[s] spectrum allocation for non-federal users."[59] "The National Telecommunications and Information Administration (NTIA)

---

[48] *See id.*

[49] *See* William M. Lawrence & Matthew W. Barnes, *5G Mobile Broadband Technology – America's Legal Strategy to Facilitate its Continuing Global Superiority of Wireless Technology*, 31 No. 5 INTELL. PROP. & TECH. L.J. 3, 4 (May 2019).

[50] *See id.* at 5.

[51] *See id.*

[52] *See* Chris Forrester, *5G: The Space Race*, IBC365 (Feb. 10, 2020), https://www.ibc.org/trends/5g-the-space-race/5446.article.

[53] GALLAGHER & DEVINE, *supra* note 4, at 1 n.1.

[54] *Id.*

[55] HOEHN & SAYLER, *supra* note 7.

[56] *Id.*

[57] GALLAGHER & DEVINE, *supra* note 4, at 18.

[58] *Id.* at 1 n.1.

[59] *Id.* The FCC Fast Plan is part of the policy to win the 5G Race. *See* Federal Communications Commission, *The FCC's 5G FAST Plan*, FCC, https://docs.fcc.gov/public/attachments/DOC-354326A1.pdf (last visited Apr. 16, 2021). The FCC is auctioning off spectrum and trying to streamline approval from federal, state, and local governmental bodies for cell site locations. *Id.* The FCC is facilitating rules to encourage faster 5G implementation by making spectrum more available in the commercial marketplace. *Id.*

manages the spectrum for federal users."[60] The NTIA works with the Department of Commerce to create a "National Spectrum Strategy."[61]

These federal agencies provide spectrum to support 5G technology. With increasing spectrum availability, more industries can access the speeds that provoke innovation. One major area of innovation affected by 5G is wearable technology.

ii. Wearable Technology and the Internet of Things

"Wearable technologies are networked devices that can collect data, track activities, and customize experiences to users' needs and desires."[62] Some future wearable technologies include nail polishes with microchips that allow users to draw virtually in 3D, buttons that provide location services, and earrings that track users' health.[63] Examples of current wearable technologies include virtual reality applications, medical devices like wearable diabetic sensors, smart yoga assistants, Apple watches, and smart compression shirts.[64] Current leaders in the wearable technology market include Fitbit, Apple, Samsung, Xiaomi, and Huawei.[65]

5G networks expand "consumer services, support the growing number of connected devices, support new industrial uses, perform advanced data analytics, and enable the use of advanced technologies."[66] The collection of these internet-connected devices creates the Internet of Things, a giant network of devices with "embedded sensors that collect and share data through closed private internet connections."[67] Smart cities use the Internet of Things to "drive economic growth, increase operational efficiencies, share information publicly, improve government services, and enhance public welfare."[68]

---

[60] GALLAGHER & DEVINE, *supra* note 4, at 1 n.1.

[61] *See id.* at 18; *see also* National Telecommunications and Information Administration, *National Spectrum Strategy*, NTIA (2019), https://www.ntia.doc.gov/category/national-spectrum-strategy.

[62] *See* Thierer, *supra* note 12, at 1.

[63] *See* Gee et. al., *supra* note 1.

[64] *See id.*; DAYDREAM, https://arvr.google.com/daydream/ (last visited Apr. 20, 2021) (virtual reality headset); INNOVOSENS, http://www.innovosens.com/about.html (last visited Apr. 19, 2021) (wearable diabetes sensor that monitors various health data for personalized treatment); YOGANOTCH, https://yoganotch.com (last visited Apr. 19, 2021) (yoga wearable assistant); *Zephyr Performance Systems*, MEDTRONIC, https://www.zephyranywhere.com (last visited Apr. 19, 2021) (wearable compression shirt that monitors users' biometrics like heart rate, G-force, and core body temperature).

[65] *See* IDC, *Market Share of Wearables Unit Shipments Worldwide By Vendor From 2014 to 2019*, STATISTA https://www.statista.com/statistics/515640/quarterly-wearables-shipments-worldwide-market-share-by-vendor/ (last visited Apr. 18, 2021).

[66] GALLAGHER & DEVINE, *supra* note 4, at "Summary".

[67] *See* Lawrence & Barnes, *supra* note 49, at 3.

[68] *See id.* at 4.

Data privacy is a significant problem with the Internet of Things. Companies can track individuals or aggregations of people wearing technologies across devices and platforms, providing companies the ability to track and monitor every person's movements.[69] For example, during the COVID-19 Pandemic, tech firms used location-tracking from users' phone data to determine popular points of interest and business activity.[70] Government officials, like California's Governor Newsom, used this information in deciding whether to tighten COVID restrictions.[71]

Advances fueled by 5G make the wearable technology field more attractive to consumers. However, these advances also make wearable technology more dangerous because whoever controls the 5G market has power; thus, foreign intelligence can manipulate perceptions and behavior. Foreign nations can collect medical data, location information, and voluntary information like names and addresses for billing.

5G wearable technology creates national security concerns. Congress restricted federal agencies from purchasing specific foreign-made telecommunications equipment.[72] Investigators found evidence of backdoors or security vulnerabilities in a variety of devices.[73] Some 5G technology uses 4G LTE as a starting point to build upon, and these "legacy issues" in 4G LTE are being carried into future technology, too, providing even more vulnerabilities.[74]

These vulnerabilities in wearable technology can be mitigated or exacerbated depending on who controls the 5G market. Thus, countries around the world are racing to control 5G.

iii. Race to 5G

The Race to 5G is the competition to develop 5G products and capture the global 5G market.[75] Companies who market 5G first have first-mover advantages like capturing more revenue and yielding long-term economic benefits for themselves and their countries.[76] The U.S. wants to

---

[69] Sam Schechner et. al., *Tech Firms Are Spying on You. In a Pandemic, Governments Say That's Okay,* WALL ST. J. (June 15, 2020), https://www.wsj.com/articles/once-pariahs-location-tracking-firms-pitch-themselves-as-covid-sleuths-11592236894.

[70] *See id.*

[71] *See id.*

[72] *See* GALLAGHER & DEVINE, *supra* note 4, at "Summary".

[73] *See* Milo Medin & Gilman Louie, *The 5G Ecosystem: Risks & Opportunities for DoD*, DEF. INNOVATION BD. (Apr. 3, 2019), https://media.defense.gov/2019/Apr/03/2002109302/-1/-1/0/DIB_5G_STUDY_04.03.19.PDF.

[74] Cybersecurity and Infrastructure Security Agency, *Overview of Risks Introduced By 5G Adoption in the United States*, CISA (Jul. 31, 2019), https://www.cisa.gov/sites/default/files/publications/19_0731_cisa_5th-generation-mobile-networks-overview_0.pdf.

[75] *See* GALLAGHER & DEVINE, *supra* note 4, at 7.

[76] *See id.* at 2.

protect national and local interests that can "provide significant consumer benefits, help to modernize industries, give U.S. companies an advantage in the global economy, and yield long-term economic gains."[77]

Before 5G, there was 4G LTE, 4G, 3G, 2G, and 1G. "G" means "Generation," a standard "built to achieve certain levels of performance" like "certain levels of speed, higher capacity, added features."[78] Capacity is "the ability of the network to carry information or calls."[79] Each new generation increased capacity. 1G provided the first mobile phone, but it was limited to voice, had limited coverage and capacity, and was not affordable.[80] 2G provided digital networks, voice, texting, and more affordable pricing.[81] 3G provided "voice, data, and mobile access to the internet," supporting smartphones and computers.[82] 4G increased speed and mobile broadband, supported entertainment streaming, mobile apps, and unlimited data plans.[83] The LTE standard (long-term evolution) "redefined network architecture to offer faster speeds and higher capacity."[84]

For 4G, U.S. companies were the leaders and drove industry standards. Because U.S. companies had the first-mover advantage, they generated $100 billion to the U.S. economy and significant economic and consumer benefits.[85] 4G contributed to "a 70% growth in the wireless industry in 2011-2014."[86] The private industry leads the 5G deployment in the U.S.[87] There is not U.S. government control of the 5G race, but the U.S. government supports the private industry by auctioning spectrum and streamlining the process to install 5G infrastructure.[88]

B. U.S. Laws Regulating 5G Wearable Technology

In an attempt to mitigate the risks caused by the Race to 5G, the U.S. has utilized CFIUS and its review power over foreign investment. First, this section will evaluate CFIUS and FIRRMA. Next, this section will analyze the benefits and detriments to CFIUS. Then, this section will discuss other laws and agencies relevant to 5G wearable technology.

---

[77] *See id.* at "Summary."
[78] *See id.* at 2.
[79] *See id.*
[80] *See id.*
[81] *See id.*
[82] *See id.*
[83] *See id.*
[84] *See id.*
[85] *See id.* at 8.
[86] *How America's Leading Position In 4G Propelled the Economy,* RECON ANALYTICS, (2018), https://api.ctia.org/wp-content/uploads/2018/04/Recon-Analytics_How-Americas-4G-Leadership-Propelled-US-Economy_2018.pdf.
[87] *See* GALLAGHER & DEVINE, *supra* note 4, at "Summary".
[88] *See id.*

i. CFIUS and the Foreign Investment Risk Review Modernization Act (FIRRMA)

In 1975, President Gerald Ford established an inter-agency committee, CFIUS, to monitor the national security impact of foreign investments in U.S. businesses.[89] CFIUS is "an interagency committee authorized to review certain transactions involving foreign investment in the U.S. ("covered transactions"), in order to determine the effect of such transactions on the national security of the U.S."[90] CFIUS reviews "certain transactions involving foreign investment in the [U.S.] and certain real estate transaction by foreign persons…."[91]

Foreign investment is "typically a good thing for the recipient country."[92] In 2019, Chinese foreign investment in the U.S. was $4.8 billion.[93] At its peak in 2016, Chinese investment in the U.S. was at $46.5 billion.[94] 92% of these billions of dollars were invested into acquisitions of American companies and intellectual property.[95] Chinese investment is made for many commercial and profit-seeking reasons. However, the Chinese government may be directing Chinese investment into strategic technologies to advance its economic and technological goals.[96] These strategic investments may be detrimental to U.S. national security and data privacy.[97]

In response to the growing concerns from Chinese foreign investment, on August 13, 2018, Congress passed, and President Trump signed the Foreign Investment Risk Review Modernization Act of 2018 (FIRRMA) into law.[98] FIRRMA expands the jurisdiction of CFIUS to address growing national security concerns over foreign exploitation of targeted investment structures and modernize the CFIUS review process. [99]

---

[89] *See* Exec. Order. No. 11,858, 3 C.F.R. § 990 (1971-1975). CFIUS operates under section 721 of the Defense Production Act of 1950, as amended, and as implemented by Executive Order 11858, as amended, and regulations 31 C.F.R. Part 800 and 31 C.F.R. Part 801.

[90] *See id.*

[91] *See id.*; *The Committee on Foreign Investment in the United States (CFIUS),* U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius (last visited Apr. 16, 2021).

[92] TOM COTTON, BEAT CHINA: TARGETED DECOUPLING AND THE ECONOMIC LONG WAR, 16 (2021), https://www.cotton.senate.gov/imo/media/doc/210216_1700_China%20Report_FINAL.pdf.

[93] *See id.*

[94] *See id.*

[95] *See id.*; *The US-China Investment Hub*, RHODIUM GRP., https://www.us-china-investment.org/fdi-data (last visited Apr. 16, 2021).

[96] *See id.*

[97] *See id.* at 5.

[98] *See id.* at 58.

[99] *See Summary of the Foreign Investment Risk Review Modernization Act of 2018*, U.S. DEP'T TREASURY, https://www.treasury.gov/resource-center/international/Documents/Summary-of-FIRRMA.pdf.

Under FIRRMA, the Department of the Treasury first introduced a Pilot Program that required mandatory CFIUS review of certain foreign investments in companies in twenty-seven industries.[100] Parties to transactions involving investments in companies outside of the twenty-seven industries were subject only to voluntary CFIUS notification requirements.[101] Companies had to self-identify whether they were part of the twenty-seven industries based on their choice of a North American Industry Classification System (NAICS) code.[102] The Pilot Program ended in February 2020, at which time the mandatory review requirement was expanded beyond the twenty-seven industries and the reliance on a NAICS codes designation that was subject to self-classification issues.[103] Now, the mandatory declaration provision includes certain foreign investment transactions involving any U.S. business that "produces, designs, tests, manufactures, fabricates, or develops one or more 'critical technologies.'"[104] Additionally, even if companies do not elect for voluntary review, CFIUS may unilaterally review a foreign investment transaction in its discretion.[105]

CFIUS's review process has been subject to criticism. Some argue it created an "air of hostility" between the U.S. and China, hurting foreign investment and relationships.[106] To understand the problems in the review process, the following subsections will explain each step of the CFIUS process, then show the review in practice.

a. The CFIUS Process

For parties to a transaction to decide whether a transaction is subject to CFIUS review, they must determine whether the CFIUS review is mandatory or voluntary. This requires the parties to determine whether the transaction involves (1) a foreign person; (2) a U.S. business; (3) a foreign person gaining control or non-controlling rights of concern with respect to the U.S. business; and (4) the U.S. business is engaged in various activities relating to critical technologies or a foreign government has a substantial interest in the foreign person and the U.S. business fits within defined critical technology, critical infrastructure, or sensitive personal data categories.[107] If

[100] *See Fact Sheet: Interim Regulations for FIRRMA Pilot Program* (Oct. 10, 2018), U.S. DEP'T TREASURY, https://home.treasury.gov/system/files/206/Fact-Sheet-FIRRMA-Pilot-Program.pdf [hereinafter Treasury Fact Sheet].

[101] *Id.*

[102] *Id.*

[103] *See* Committee on Foreign Investment in the United States, *CFIUS Annual Report to Congress*, U.S. DEP'T TREASURY, at *iv.* (2019), https://home.treasury.gov/system/files/206/CFIUS-Public-Annual-Report-CY-2019.pdf.

[104] 31 C.F.R. 800.401(c)(1) (2020).

[105] *Id.*

[106] *See* Andrew Thompson, *The Committee on Foreign Investment in the United States: An Analysis of the Foreign Investment Risk Review Modernization Act of 2018*, 19 J. HIGH TECH. L. 361, 406 (2019).

[107] 31 C.F.R. § 800.401 (2020).

the transaction involves all four, then the transaction parties must file a mandatory declaration with CFIUS. The parties can also choose to file voluntarily, or CFIUS can, on its own, launch a review. Once subject to the CFIUS review, CFIUS will examine the transaction for natural security concerns subject to a statutorily mandated timeline: there is a 45-day review period and a 45-day investigation period, followed by a 15-day period for presidential action.[108]

The first question to ask to determine whether a CFIUS review is mandatory is whether the buyer or investor is a foreign person.[109] A foreign person includes a foreign national, a foreign entity (not including where U.S. nationals own a majority equity interest), or "any entity, foreign or domestic over which control is exercised or exercisable" by the foreign entity.[110]A U.S. company controlled by foreign parties may be subject to review.[111] If the buyer or investor is not a foreign person, then a mandatory declaration is not required.[112]

Suppose the buyer or investor is a foreign person. In that case, the second question to ask to determine if a declaration is mandatory is whether the foreign person is obtaining an interest in a U.S. business. A "U.S. business" is "any entity, irrespective of the nationality of the persons that control it, engaged in interstate commerce in the [U.S.]."[113]

If a foreign person is obtaining an interest in a U.S. business, the third question is whether the transaction would result in the foreign business obtaining "control" or "non-control rights of concern" in the U.S. business. FIRRMA broadly defines "control" as,

> the power, direct or indirect, whether or not exercised, through voting interest or otherwise, to determine, direct, or decide important matters affecting an entity, subject to regulations prescribed by [CFIUS].[114]

Rights of concern include: (1) board membership, observer, or nomination rights; (2) involvement, other than through voting of shares, in substantive decision-making regarding: (i) use, development, acquisition, safekeeping, or release of sensitive personal data of U.S. citizens; (ii) use, development, acquisition, or release of critical technologies; or (iii) management, operation,

---

[108] 31 C.F.R. §§ 800.502, 800.505; 800.508 (2020); 31 C.F.R. § 802.508 (2020); *see CFIUS Overview,* U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-overview (last visited Apr. 16, 2021). There may be extensions in certain circumstances. *Id.*

[109] 31 C.F.R. §§ 800.224, 800.301 (2020).

[110] 31 C.F.R. § 800.224 (2020).

[111] 31 C.F.R. § 800.401 (2020).

[112] *See id.*

[113] 31 C.F.R. § 800.252 (2020).

[114] 50 U.S.C. § 4565(a)(3); 31 C.F.R. § 800.208 (2020).

manufacture, or supply of critical infrastructure; and (3) access to material non-public technical data in the possession of the U.S. business.[115]

If the foreign person does obtain control or non-controlling rights of concern in the U.S. business, the fourth question is whether the U.S. business involves 1) critical technologies; 2) critical infrastructure; 3) sensitive personal data; or 4) national security concerns. The company must determine on its own whether its transaction involves any of these four. Each will be discussed below.

"Critical technologies" covers five different areas incorporating other laws: 1) items on the U.S. Munitions List; 2) items on the Commerce Control List pursuant to multilateral regimes or based on unilateral controls for regional stability, surreptitious listening; 3) emerging and foundational technologies added to the Commerce Control List; 4) nuclear-related items covered by 10 C.F.R. §§ 110 or 810; and 5) select agents and toxins covered by various laws.[116]

If critical technologies *are* at issue, the next question is whether U.S. export authorization is required to export the critical technologies to foreign persons or parties with a direct or indirect voting interest of 25% or more in the foreign person. If export authorization is required, then the company must file a mandatory declaration subjecting itself to CFIUS review.[117] If there is no export authorization, but critical technologies are at issue, the company may still need to file a mandatory declaration if the foreign person will obtain a voting interest of 25% or more in the U.S. business and a foreign government entity has a voting interest of 49% or more in the foreign person.

If there are no critical technologies at issue, a mandatory declaration may still be required if the U.S. business performs critical infrastructure functions which generally relates to communications services connected to the military; finance; transportation; oil and gas; electricity; water; and defense *and* the foreign person will obtain a voting interest of 25% or more in the U.S. business and a foreign government entity has a voting interest of 49% or more in the foreign person.[118]

If the U.S. business performs critical infrastructure functions, the next question is whether the U.S. business directly or indirectly collects or maintains "sensitive personal data" of U.S. citizens.[119] Sensitive personal data is defined by FIRRMA but focuses on whether the information is targeted to government agencies with security functions of data of over one

---

[115] 31 C.F. R. §§ 800.211, 800.401 (2020).

[116] 31 C.F.R. § 800.215 (2020).

[117] There are exceptions for certain countries. 31 C.F.R. § 800.218 (2020); *see also CFIUS Excepted Foreign States*, U.S. DEP'T TREASURY, https://home.treasury.gov/policy-issues/international/the-committee-on-foreign-investment-in-the-united-states-cfius/cfius-excepted-foreign-states (last visited Apr. 25, 2021).

[118] *See id.*

[119] 31 C.F.R. §§ 800.241, 800.401 (2020).

million individuals.[120] Even if there is sensitive personal data, a review may still be voluntary if the foreign person does not obtain a voting interest of 25% or more or a foreign government entity does not have a voting interest of 49% or more in the foreign person.[121]

If there is no sensitive personal data at issue, the next question is whether the foreign person's investment presents any other national security concerns.[122] "National security" is not defined and is more of a totality of the circumstances test depending on the type of technology, the key suppliers to the U.S. government, the proximity to sensitive infrastructure, and access to citizens' personal information.[123] If it does, a review is merely voluntary.

There are certain exceptions from mandatory filing requirements for certain investors from the U.K., Canada, and Australia and for investment funds that satisfy certain conditions regarding foreign partners.[124]

If a business voluntarily files or is subject to mandatory filing, CFIUS launches an investigation into the national security of the businesses and their effect on the U.S.[125] These investigations may last months.[126] CFIUS review has been called a "legal black hole" as it does not release the results of its investigations.[127] Ultimately, CFIUS will provide a report and recommendation to the President about whether to allow or block a transaction. It is unlikely that a company will want to subject itself to months long CFIUS investigations. However, if a company chooses not to file a voluntary review, it may still be subject to a retroactive review. These reviews can be very costly and lengthy and may cause past transactions to be undone.

b. CFIUS Review in Practice

In practice, CFIUS blocks acquisitions, takeovers, and mergers that involve foreign investors posing a risk to national security.[128] To show how CFIUS's review works, this comment will describe recent applications, especially highlighting the Broadcom Acquisition and the TikTok acquisition.

When Broadcom, a Singapore company, sought to acquire Qualcomm, a U.S. company, the technology companies fought over the

---

[120] *Id.*

[121] *Id.*; *see* JACKSON, *supra* note 24, at 13.

[122] *Id.*

[123] *See* Christopher M. Tipler, *Defining National Security: Resolving Ambiguity in the CFIUS Regulations*, 35 U. PA. J. INT'L L. 1223, 1251 (2014).

[124] *See* 31 C.F.R. § 800.218 (2020); *see also CFIUS Excepted Foreign States*, *supra* note 117.

[125] *See id.*

[126] *See* JACKSON, *supra* note 24, at 13-14.

[127] Ji Li, *Investing Near the National Security*, 14 BERKELEY BUS. L.J. 1, 6 (2017).

[128] *See* Westbrook, *supra* note 25, at 643.

acquisition.[129] Broadcom was acquiring proxies to elect a majority of the Board of Directors in Qualcomm to approve a merger.[130] Qualcomm did not want this hostile takeover.[131] Broadcom tried to redomicile in Delaware to avoid CFIUS review.[132] However, Qualcomm filed a voluntary notice to CFIUS in an effort to stop the takeover.[133] CFIUS launched an investigative review into Broadcom's connection with third-party foreign entities and the national security effects of its intentions.[134] CFIUS concluded that the takeover of Qualcomm would weaken its position in U.S. 5G technology, opening a door for Chinese companies to "compete robustly" in the 5G standard-setting process.[135] This takeover would contribute to Chinese 5G dominance which would have "substantial negative national security consequences for the [U.S]."[136] In 2018, CFIUS recommended that President Trump block the acquisition to protect national security, which he did by executive order. [137]

Even more recently than Broadcom, CFIUS reviewed a 2017 transaction regarding Chinese company ByteDance's acquisition of Musical.ly, a U.S. social media app.[138] In 2018, ByteDance merged Musical.ly with its TikTok app.[139] TikTok rapidly rose in popularity in 2019 with its short videos capturing the attention of millions of people globally, especially U.S. users.[140] Using its discretion, in 2019, two years after the acquisition, CFIUS opened an investigation because of the national security concerns regarding China's access to U.S. user data.[141] During the summer of 2020, President Trump considered banning TikTok from the U.S., a move other countries like India had already taken.[142] Companies such as Walmart, Oracle, and Microsoft began negotiations with ByteDance to acquire TikTok which would avoid any ban.[143] On August 14, 2020, President Trump issued an Executive Order ordering ByteDance, to divest all of its interest in TikTok

---

[129] *See id.* at 652-53.
[130] *See id.* at 652.
[131] *See id.* at 653-54.
[132] *See id.* at 652.
[133] *See id.* at 653.
[134] *See id.* at 654; *see also* Letter from Aimen N. Mir, Deputy Assistant Sec'y Inv. Sec., Dep't Treasury, to Mark Plotkin & Theodore Kassinger (Mar. 5, 2018), http://online.wsj.com/public/resources/documents/cfiusletter.pdf.
[135] *See* Westbrook, *supra* note 25, at 655-56.
[136] *See id.* at 656. CFIUS's national security reasons were kept confidential, but President Trump identified Qualcomm's importance in developing 5G and its relationship with the U.S. Defense Department. *See id.*
[137] *See id.* at 658.
[138] *TikTok Is Running out of Time: Understanding the CFIUS Decision and Its Implications,* CSIS (Sep. 2, 2020), https://www.csis.org/analysis/tiktok-running-out-time-understanding-cfius-decision-and-its-implications.
[139] *Id.*
[140] *Id.*
[141] *Id.*
[142] *Id.*
[143] *Id.*

within 90 days.[144] President Trump's order was based upon CFIUS's findings during their review.[145] During the 2020 election, President Biden's campaign staff were not allowed to use TikTok and had to remove the app from their phones.[146] President Trump also issued an executive order about WeChat, "a messaging, social media, and electronic application owned by the Chinese company Tencent Holdings Ltd."[147] Similarly, in March 2019, CFIUS ordered Kunlun Tech to divest Grindr over national security and privacy concerns about access to personal data.[148]

ii. Other Relevant Laws and Privacy Concerns

Other than the CFIUS-FIRRMA scheme, the U.S. has other relevant laws to address this problem of national security and data privacy threats. This section will give a brief overview of Team Telecom, the Secure 5G and Beyond Act, the FCC Fast Plan, and state laws.[149]

---

[144] *Id.*; *see generally* Exec. Order No. 13942, 85 Fed. Reg. 48637 (2020), https://www.federalregister.gov/documents/2020/08/11/2020-17699/addressing-the-threat-posed-by-tiktok-and-taking-additional-steps-to-address-the-national-emergency.

[145] *See id.* This order was challenged by ByteDance and is now under review. *See* Noah Manskar, *TikTok Deal With Oracle, Walmart Reportedly Put On Hold Under Biden*, NEW YORK POST (Feb. 10, 2021), https://nypost.com/2021/02/15/bytedance-reportedly-scraps-deal-to-sell-tiktok-to-oracle/. After President Biden won the election, ByteDance pulled out of its arrangement with Oracle and Walmart. *See id.* The Biden Administration now has this on pause. *See id.*; *see also* Echo Wang & David Shepardson, *China's ByteDance Challenges Trump's TikTok Divesture Order*, REUTERS (Nov. 11, 2020), https://www.reuters.com/article/usa-tiktok/chinas-bytedance-challenges-trumps-tiktok-divestiture-order-idUSKBN27R07W.

[146] *See* Sarah Mucha, *Biden Campaign Tells Staff to Delete TikTok From Their Phones*, CNN (Jul. 28, 2020), https://www.cnn.com/2020/07/28/politics/biden-campaign-tiktok/index.html.

[147] Exec. Order No. 13943, 85 Fed. Reg. 48641 (Aug. 11, 2020), https://www.federalregister.gov/documents/2020/08/11/2020-17700/addressing-the-threat-posed-by-wechat-and-taking-additional-steps-to-address-the-national-emergency.

[148] *Id.* One of the major concerns with Grindr, a dating app, was the possibility that the Chinese would steal personal data and blackmail citizens. COTTON, *supra* note 92, at 22.

[149] There are many other relevant laws related to this topic, but outside the scope of this comment. The International Emergency Economic Powers Act "provides the President with broad authority to take adverse economic actions upon a finding of a national emergency." Jonathan Wakely & Andrew Indorf, *Managing National Security Risk in an Open Economy: Reforming the Committee on Foreign Investment in the United States*, 9 HARV. NAT'L SEC. J. 1, 10 (2018) (The President can "prevent or prohibit, any acquisition, holding . . . use, transfer . . . importation or exportation of . . . any property in which a foreign country or national thereof has an interest."). 50 U.S.C. § 1702. Another relevant law, or lack thereof, is data privacy. The U.S. does not have an extensive data privacy scheme like Europe. The European Union's General Data Protection Regulation (GDPR) protects personal data, any information related to an identified or identifiable living individual. *See* European Commission, *Data Protection in the EU,* (2019), https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en. While the U.S. has data privacy laws, they are not as extensive or protective. Additionally, the Federal Trade Commission (FTC) also can investigate companies that violate U.S. privacy laws. Exec. Order No. 13942, 85 Fed. Reg. 48637 (Aug. 6, 2020). The FTC began investigating TikTok's alleged violations of U.S. privacy law in July 2020. *Id.* While

The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector, also known as "Team Telecom," is a committee of the head of Justice, Defense, and Homeland Security with the Attorney General as the head.[150] Team Telecom assists the FCC by reviewing telecom license applications, deals, and other requests made to the FCC for "national security and law enforcement concerns that may be raised by foreign participation in the [U.S.] telecommunications services sector."[151] While similar to CFIUS in its goals to protect national security, Team Telecom mainly focuses on telecommunications rather than investment in businesses from foreign persons that may raise concerns.[152] As Team Telecom is still in the initial stages of its formalization, it is too early to understand its full power. However, it will likely become more prevalent in the coming years.[153]

The Secure 5G and Beyond Act requires "the President to develop a 5G protection strategy."[154] President Trump's strategy was released in March 2020.[155] The FY2020 National Defense Authorization Act similarly requires the Department of Defense's Secretary of Defense to develop a 5G strategy, which was released in May 2020.[156] As part of his strategy, President Trump created the Cybersecurity and Infrastructure Security Agency (CISA) to lead 5G risk management efforts.[157] CISA's national strategy is to "facilitate domestic 5G rollout, assess risks to and identify core security principles of 5G infrastructure, address risks to [U.S.] economic and national security during development and deployment of 5G infrastructure worldwide, and promote responsible global development and deployment of 5G."[158] CISA acts as an adviser and partner to private industries in an effort to secure 5G.

The U.S. faces both federal and state barriers to 5G implementation. 5G deployment suffers from "[a] lengthy spectrum allocation process, resistance from local governments to federal small cell siting rules, and

---

encouraging, these laws are retrospective and do not work to protect U.S. data theft before it occurs.

[150] Process Reform for Executive Branch Review of Certain FCC Applications and Petitions Involving Foreign Ownership, 85 Fed. Reg, 76360, 76361 (Nov. 27, 2020); Exec. Order No. 13913, 85 Fed. Reg. 19643, 19643-44 (Apr. 4, 2020).

[151] *Id.* at 76361.

[152] National Security Division, *The Committee for the Assessment of Foreign Participation in the United States Telecommunications Services Sector – Frequently Asked Questions*, U.S. DEP'T JUSTICE, (last updated Apr. 23, 2020), https://www.justice.gov/nsd/committee-assessment-foreign-participation-united-states-telecommunications-services-sector#11; *see also* Report and Order, FCC 20-133, 1, 7 (2020), https://docs.fcc.gov/public/attachments/FCC-20-133A1.pdf

[153] Report and Order, F.C.C. 20-133, 1, 79 (2020).

[154] HOEHN & SAYLER, *supra* note 7.

[155] *See id*.

[156] *Id.*

[157] U.S. DEP'T OF HOMELAND SEC., CISA 5G STRATEGY ENSURING THE SECURITY AND RESILIENCE OF 5G INFRASTRUCTURE IN OUR NATION 1 (2020).

[158] *Id*. at 3.

limitations on trade that may affect the availability of equipment."[159] More than 20 states have passed small cell laws.[160]

Some small cell laws limit collection rates and public right-of-way access fees.[161] Some laws restrict or limit municipal ordinances.[162] Others dictate how cities may regulate small cell deployments.[163] Municipal regulations are ill-equipped to facilitate small cell deployments because they lack the uniformity needed from one municipality to another.[164] The FCC in 2020 responded to these state issues by interpreting the Telecommunications Act of 1996 as giving the FCC's regulations preemption over local regulations that prohibited small cell wireless structures.[165]

Export control schemes are also relevant because CFIUS relies on them to determine which critical technologies are required to file disclosures. Under the Export Administration Regulations (EAR), as administered by the Bureau of Industry and Security (BIS), certain commercial products, dual-use commercial and military products, and certain designated munitions items with some use in the military are subject to licensing requirements.[166] About 95% of exported items do not require an export license.[167] The International Traffic in Arms Regulations (ITAR) applies to the export of defense articles, technical data, or defense services designated on the U.S. Munitions List.[168]

The ITAR and EAR schemes have a long history of uncertainty. Companies self-identify their jurisdiction and classification but often are not sure which regulatory scheme they fall under.[169] Many companies contact the government every year questioning how to classify their products.[170] The recent U.S. government's export control reform has not made the process easier. The rules are likely more impactful on smaller businesses that do not

---

[159] *See* GALLAGHER & DEVINE, *supra* note 4, at "Summary".

[160] *See* Lawrence & Barnes, *supra* note 49, at 5-6.

[161] *See id.*

[162] *See id.*

[163] *See id.*

[164] *See id.* at 7.

[165] City of Portland v. United States, 969 F.3d 1020, 1041, 1053 (9th Cir. 2020) (upholding the FCC's interpretation); *see 5G will Change the World: China Wants to Lead the Way*, CNET, https://www.cnet.com/news/5g-will-change-the-world-and-china-wants-to-lead-the-way/ (last visited Apr. 18, 2021).

[166] *Export Licensing,* EXPORT.GOV., https://www.export.gov/article2?id=Export-Licensing (last visited Apr. 18, 2021).

[167] *Id.*

[168] 22 C.F.R. § 120.2 (2013).

[169] U.S. DEP'T OF COMMERCE BUREAU OF INDUS. AND SEC., ANNUAL REPORT TO CONG. FOR FISCAL YEAR 2020, 10 (2020) [hereinafter Bureau Annual Report]; *Export Control Reform: Challenges for Small Business? (Part I): Hearing Before the Subcomm. on Agriculture, Energy and Trade of the Comm. on Small Business*, 114th Cong. 20 (2016) (statement of Andrea Appell). In 2020, the BIS processed 3,128 classifications request applications. *See* Bureau Annual Report, *supra*, at 10.

[170] Bureau Annual Report, *supra* note 169, at 10.

have the resources or knowledge about these schemes.[171] As discussed infra, the CFIUS definition of "critical technology"–reliant on the export control system–creates an inherently complex system rife with errors.

Another way Congress is trying to mitigate risks is through laws banning foreign-made telecommunications equipment. Congress passed the John S. McCain National Defense Authorization Act for Fiscal Year 2019.[172] The Act included FIRRMA, but it also restricts federal agencies from purchasing specific foreign-made telecommunications equipment.[173] It prohibits federal agencies' heads from procuring telecommunications from Huawei, ZTE Corporation, and other telecommunications companies.[174] On March 12, 2020, President Trump signed the Secure and Trusted Communications Networks Act of 2019, which has three main parts, the law: (1) prohibits "the FCC from subsidizing the acquisition or maintenance of telecommunications equipment or services from untrusted suppliers;" (2) creates "a program to reimburse telecommunications providers with fewer than two million customers to remove equipment that poses a national security risk and replace it with trusted supplier equipment;" and (3) establishes "an information sharing program for telecommunications providers, particularly small and rural operators, to obtain information regarding potential security risks and vulnerabilities to their networks."[175]

While these laws provide some protections from Chinese interference, they do not protect data in situations where we do not trade the product but where we develop it in the U.S. and have foreign investment.

C. Chinese Threat to U.S. Data

In a 2017 Report to the President, "Ensuring Long-Term U.S. Leadership in Semiconductors," the Executive branch recognized that "Chinese policies are distorting markets in ways that undermine innovation, subtract from U.S. market share, and put U.S. national security at risk."[176] "Each country[] adopt[s] a different strategy to lead in 5G technology development and deployment."[177] "China has a national plan to deploy 5G

---

[171] *Id.* at 21-22. BIS is attempting to help smaller businesses by providing education and counseling.

[172] John S. McCain National Defense Authorization for Fiscal Year 2019, 115 Pub. L. No 232, 132 Stat. 1636.

[173] *See* GALLAGHER & DEVINE, *supra* note 4, at 1.

[174] *Id.*

[175] *Senate Passes Secure and Trusted Communications Networks Act*, INSIDE TOWERS (Feb. 28, 2020), https://insidetowers.com/cell-tower-news-senate-passes-secure-and-trusted-communications-networks-act/; Secure and Trusted Communications Networks Act of 2019, Pub. L. No. 116-124, 134 Stat. 158 (2020).

[176] PRESIDENT'S COUNCIL OF ADVISORS ON SCIENCE AND TECHNOLOGY, ENSURING LONG-TERM U.S. LEADERSHIP IN SEMICONDUCTORS, 2 (Jan. 2017), https://obamawhitehouse.archives.gov/sites/default/files/microsites/ostp/PCAST/pcast_ensuring_long-term_us_leadership_in_semiconductors.pdf.

[177] *See* GALLAGHER & DEVINE, *supra* note 4, at "Summary".

domestically, capture the revenues from its domestic market, improve its industrial system, and become a leading supplier of telecommunications equipment to the world."[178] This section will discuss China's plan for 5G dominance and then will discuss how China's plan is being implemented through a discussion on Huawei.

i. China's Plan for 5G Dominance

China has affirmed its plan for 5G Dominance through its initiatives. In 2013, China launched *One Belt, One Road* to expand its global economic reach and influence.[179] To further its goals, in 2015, China implemented its 13th Five-Year Plan for Economic and Social Development of China, more commonly referred to as "Made in China 2025."[180] Made in China 2025 is a national plan to launch 5G by 2020.[181] While China has made considerable deployments of 5G, as of 2021, it has yet to implement a nationwide 5G infrastructure successfully. China has made advancements in its plan by "investing in [research and development], participating, and leading in 5G standards development to benefit Chinese firms, engaging in international 5G projects to build knowledge, building capacity to provide 5G equipment, and reserving spectrum for 5G use."[182] Since the Made in China Plan 2025 was implemented in 2015, China invested $400 billion in 5G, outspending the U.S. by $24 billion.[183] China has "built 350,000 new cell sites, while U.S. companies have built 30,000 in the same timeframe."[184]

To help 5G technology grows, China has "provided $400 billion in 5G investments, coordinated with companies manufacturing 5G technologies, and worked with Chinese providers to deploy 5G infrastructure…"[185] China is deploying 5G domestically with plans to capture revenues from its market, upgrade its industrial system, "build its capacity to develop technology equipment and components," and "become a leading supplier of 5G technologies to the world."[186] In October 2020, China's Central Committee "reaffirmed the effort's central role in national economic development and securing China's supply chains."[187]

---

[178] *Id.*

[179] KAREN M. SUTTER ET.AL., CONG. RESEARCH SERV. IF11735, CHINA'S "ONE BELT, ONE ROAD" INITIATIVE: ECONOMIC ISSUES, 1 (Jan. 22, 2021).

[180] Central Committee of the Communist Party of China, *The 13th Five-Year Plan for Economic and Social Development of the People's Republic of China*, CENTRAL COMPILATION AND TRANSLATION PRESS (2015), http://en.ndrc.gov.cn/newsrelease/201612/P020161207645765233498.pdf.

[181] *See* GALLAGHER & DEVINE, *supra* note 4, at 8-9.

[182] *See id.* at 9.

[183] *See id.* at 10.

[184] *See id.* at 10.

[185] *See id.* at 8.

[186] *See id.* at 9.

[187] SUTTER ET AL., *supra* note 179, at 1.

ii. Chinese Investments and Control of 5G Exemplified with Huawei

China's plan for domination can be exemplified through Huawei, one of China's most significant threats to the U.S.[188] Huawei is a major Chinese telecommunications company.[189] Huawei and other Chinese companies are under the control of the Chinese government.[190] China's National Intelligence Law, enacted in June 2017, requires "any organization and citizen, shall in accordance with the law, support, provide assistance, and cooperate in national intelligence work, and guard the secrecy of any national intelligence work that they are aware of."[191] This law means that Chinese telecom operators must provide Chinese intelligence services or military access to technology or services.[192] Even companies from other foreign countries or companies that have Chinese controlling shareholders may also be subject to Chinese control.[193] Such unfettered access to these networks concerns major data privacy issues.

Huawei's equipment "could endanger national security," and it is the world's biggest supplier of telecom equipment.[194] Huawei provides cheaper products than its competitors while maintaining quality.[195] Huawei is also "clouded by allegations of intellectual property theft."[196] Canadian investigations found stolen Cisco-made code in Huawei products.[197] Previous hackers stole files from Canadian telecom computer systems.[198]

---

[188] GALLAGHER & DEVINE, *supra* note 4, at 25-26.

[189] *Id.*

[190] *Id.*; HOEHN & SAYLER, *supra* note 7.

[191] *Id.*

[192] *See id.*

[193] *Id.*

[194] *See* Brian Fung, *How China's Huawei Took the Lead Over U.S. Companies in 5G Technology*, THE WASH. POST, (Apr. 10, 2019), https://www.washingtonpost.com/technology/2019/04/10/us-spat-with-huawei-explained/. Huawei's chief rivals are Nokia and Ericcson. *See id.*

[195] GALLAGHER & DEVINE, *supra* note 4, at 25-26.

[196] *See* Fung, *supra* note 194.

[197] *See id.*

[198] *See id.* The FBI says China "is seeking to become the world's greatest superpower through predatory lending and business practices, systematic theft of intellectual property, and brazen cyber intrusions." *See The China Threat,* FBI, https://www.fbi.gov/investigate/counterintelligence/the-china-threat (last visited Apr. 16, 2021). In fact, Australia determined that China hacked its parliament and political parties before its election in May 2019. Colin Packham, *Exclusive: Australia Concluded China Was Behind Hack on Parliament, Political Parties- Sources*, REUTERS (Sep. 15, 2019), https://www.reuters.com/article/us-australia-china-cyber-exclusive/exclusive-australia-concluded-china-was-behind-hack-on-parliament-political-parties-sources-idUSKBN1W00VF. While the Chinese used sophisticated hacking measures there; now any new hacking attempts would be more straightforward if the Chinese already had control of the 5G infrastructure being used. *Id*.

Huawei phones are popular around the world but "banned" in the U.S.[199] In 2012, the U.S. banned Huawei networking equipment from company use.[200] In 2019, President Trump issued an executive order banning Huawei from the U.S. communication network.[201] Shortly following the executive order, the U.S. Department of Commerce's Bureau of Industry and Security added Huawei to its Entity List, a list of foreign persons "subject to specific license requirements for export, reexport, and/or transfer (in-country) of specified items."[202] In June 2020, the FCC's Public Safety and Homeland Security Bureau designated "Huawei and ZTE as posing national security threats to the integrity of communications networks."[203] Removing and replacing all the Huawei and ZTE equipment already in U.S. networks will cost about $1.837 billion.[204] The Rip and Replace law is another way the U.S. is encouraging smaller telecommunications firms to update their equipment with funding from the FCC.[205] The U.S. is not alone in its ban on Huawei technologies. On July 14, 2020, the United Kingdom "banned Huawei from its 5G infrastructure" and ordered the equipment already installed to be removed by 2027.[206] In August 2020, India began removing Huawei's equipment from its 5G networks.[207]

While the U.S. is attempting to mitigate issues arising from Huawei and other issues of Chinese involvement, the risks are so high, and the U.S. protections could be stronger.

---

[199] *See* Sean Keane, *Huawei Ban Timeline: Company Tries to Blame US Sanctions For Global Chip Shortage*, CNET (Apr. 15, 2021), https://www.cnet.com/news/huawei-ban-full-timeline-us-sanctions-china-trump-biden-5g-phones/. While U.S. citizens may purchase and use Huawei phones, Huawei is not allowed access to Google or any of its program (other than Android's open-source network). *Id.* This effectively banned Huawei from the U.S. market, although not expressly.

[200] *Id.*

[201] *See id.*; Securing the Information and Communications Technology and Services Supply Chain, 84 Fed. Reg. 22691 (May 15, 2019), https://www.federalregister.gov/documents/2019/05/17/2019-10538/securing-the-information-and-communications-technology-and-services-supply-chain.

[202] *Entity List*, BUREAU OF INDUS. AND SEC., https://www.bis.doc.gov/index.php/policy-guidance/lists-of-parties-of-concern/entity-list (last visited Apr. 18, 2021); *Supplement No. 4 to Part 744- Entity List*, BUREAU OF INDUS. AND SEC. (Apr. 8, 2021), https://www.bis.doc.gov/index.php/documents/regulations-docs/2326-supplement-no-4-to-part-744-entity-list-4/file.

[203] Anna Veigle, *FCC Releases Results of Supply Chain Data Request*, FED. COMMUNC'NS COMM'N, (Sept. 4, 2020), https://docs.fcc.gov/public/attachments/DOC-366702A1.pdf.

[204] *Id.*

[205] *President Signs Rip and Replace Bill into Law*, U.S. SENATE COMM. COM., SCI. & TRANSP. (Mar. 12, 2020), https://www.commerce.senate.gov/2020/3/president-signs-rip-and-replace-bill-into-law.

[206] *Huawei To Be Removed from UK 5G Networks By 2027*, GOV.UK, (Jul. 14, 2020), https://www.gov.uk/government/news/huawei-to-be-removed-from-uk-5g-networks-by-2027.

[207] Keane, *supra* note 199.

III. ANALYSIS

CFIUS's mandatory declarations process does not provide adequate protection for American privacy and national security. Companies can easily circumvent CFIUS review by choosing not to voluntarily file while running the risk of CFIUS's discretionary retroactive review. The proposed solution is to strengthen the CFIUS review process by clarifying its reliance on export-control systems and requiring mandatory review based on certain terms. This comment will apply the solution to a practical problem and then analyze alternative solutions.

A. Legal Problem Analysis: CFIUS's Review Does Not Provide Adequate Protection for American Privacy and National Security

CFIUS's purpose is to protect from foreign countries gaining access to U.S. products that concern national security, but even after the FIRRMA amendments, CFIUS fails to live up to its purpose.[208] CFIUS's review does not provide adequate protection from Chinese threats to data privacy and national security because 1) CFIUS review is mostly a voluntary process and mandatory review occurs based on a company's self-classification, and 2) CFIUS relies on an export control system rife with uncertainty to define what is "critical technology" for purposes of a covered transaction.

i. Voluntary Process and Self-Classification

CFIUS review is insufficient at protecting against threats to national security and data privacy because the review is "largely a voluntary process," and its mandatory reviews are seriously limited.[209] As a mostly voluntary process, companies can very easily avoid review. Mandatory declarations for CFIUS review are only required when 1) there is a critical technology that would require export authorization, or 2) the U.S. business performs critical infrastructure functions or collects sensitive personal data, and the foreign person will obtain a voting interest of 25% or more and a foreign government entity has a voting interest of 49% or more in the foreign person. These two circumstances are extremely limited and rife with problems.

For an example of these limitations, consider the mandatory filing requirements for critical infrastructure functions and sensitive personal data. Even if it were certain for companies that they meet those standards, a mandatory filing is only required if a foreign person will obtain a voting interest of 25% and a foreign government entity having a voting interest of

---

[208] 31 C.F.R. §§ 800.224, 800.301 (2020).

[209] *Fact Sheet: Final CFIUS Regulations Implementing FIRRMA*, U.S. DEP'T TREASURY (Jan. 13, 2020), https://home.treasury.gov/system/files/206/Final-FIRRMA-Regulations-FACT-SHEET.pdf [hereinafter Fact Sheet].

49% in the foreign person. This mandatory filing requirement is easily worked around. A foreign government entity with a voting interest of 95% can invest up less than 25% and avoid a mandatory filing. Alternatively, a foreign person with a 48% voting interest from a foreign government entity could obtain 100% interest in the U.S. business without a review. This shows how a company can work around a CFIUS mandatory filing easily.

Even if companies are not purposefully trying to work around CFIUS review, companies often do not realize they are involved with critical technology, sensitive personal data, or national security concerns, and there is no law requiring they find out. This is a major hole in the review process because it is based upon a company's voluntary self-classification. If a company is not required to find out if they fall under those terms, then the voluntary process lies solely in a company's discretion.

Companies may consider voluntarily filing to avoid CFIUS initiating their own review, which can be retroactive, as in the case of ByteDance and TikTok.[210] However, with the billions of dollars invested in U.S. companies every year, it is nearly impossible for CFIUS to know every investment occurring. Additionally, even if CFIUS decided to launch a review, it could be too late for the national security risks. Once China has access to new technology, it can copy it, hack it, or leave bugs behind to find breaches in its security. There is no specific law protecting the privacy of American citizens from foreign intelligence for wearable technology.[211]

Additionally, foreign governments, like China, have laws where they can access any Chinese business. Chinese foreign persons investing in U.S. businesses can completely avoid CFIUS review even if they have sensitive personal data or other national security concerns if the Chinese government does not have a formal voting interest of over 49%. The Chinese government can still completely access every Chinese business rendering a CFIUS review almost meaningless.

Moreover, there are no protections available when a company invests in a U.S. business then sells the business to China. For example, a

---

[210] Another recent emerging issue is the national security concerns of apps. *See* Sherisse Pham, *TikTok Could Threaten National Security, US Lawmakers Say*, CNN (Oct. 25, 2019), https://www.cnn.com/2019/10/25/tech/tiktok-national-security/index.html. Even if the technology is American-owned, the Chinese can gain access to the platforms with users installing Chinese-controlled apps. *See id.* As discussed infra, on October 25, 2019, Congress called for an investigation of the popular video app TikTok. Because an app may have ties to China, or even Russia, like the app "FaceIt" that applied age filters, the app's company is subject to Chinese law, which allows for access to all of its data. *See* Kate O'Flaherty, *The FBI Investigated FaceApp. Here's What It Found*, FORBES (Dec. 3, 2019), https://www.forbes.com/sites/kateoflahertyuk/2019/12/03/fbi-faceapp-investigation-confirms-threat-from-apps-developed-in-russia/?sh=21991f6245bc.

[211] *See* Alexandra Troiano, *Wearables and Personal Health Data: Putting a Premium on Your Privacy*, 82 BROOK. L. REV. 1715, 1748 (2017). Europe has the GDPR, but the U.S. has no federal equivalent. State laws equivalents are growing, but this is outside the scope of this comment.

traditional U.S. ally may be able to invest easier into U.S. businesses avoiding CFIUS review.[212] If the ally provides China access to the business, then the business has wholly avoided CFIUS review and granted China access to massive amounts of data.[213]

The voluntariness of the filing process and reliance on self-classification for CFIUS review shows how easily a company can avoid a CFIUS review and how CFIUS needs to be strengthened to protect U.S. citizen's national security and data privacy.

ii. Uncertainty in What "Critical Technologies" Means Under an Export Controls System

Another problem with CFIUS is its reliance on export control systems to define "critical technologies." The export controls systems CFIUS relies on for its critical technologies mandatory filing criteria are rife with uncertainty. CFIUS requires mandatory review for businesses based on their identification as a transaction involving "critical technologies" as "defined to include certain items subject to export controls and other existing regulatory schemes, as well as emerging and foundational technologies controlled pursuant to the Export Control Reform Act of 2018."[214] The "critical technologies" definition is a significant flaw in FIRRMA because it depends on an export controls system not designed for or well utilized as a system for self-identification.

The export controls system has a long history of uncertainty. Companies must self-identify whether they fall into an export regime. There is not much consistency or coordination among the export regimes causing confusion about jurisdiction and inefficiencies in the process.[215] Thousands of companies contact the government every year questioning how to classify themselves.[216] Companies may choose the wrong jurisdiction or classification, either in good faith or to avoid CFIUS review. There is no working standard, and the system is very uncertain. The export controls standard was created for economic and exporting purposes in a "different era, when the distinction between civil and military technologies was clearer and there was little overlap between the economies of the [U.S.] and its competitors."[217] Now the distinctions are blurred and the economies are interconnected causing the export controls system to be uncertain.

---

[212] *See* Thompson, *supra* note 106, at 403.

[213] *See id.*

[214] Fact Sheet, *supra* note 209.

[215] *See* IAN F. FERGUSSON & PAUL K. KERR, CONG. RSCH. SERV. R41916, THE U.S. EXPORT CONTROL SYSTEM AND THE EXPORT CONTROL, REFORM INITIATIVE, 1, 1 (Jan. 28, 2020).

[216] *See* Bureau Annual Report, *supra* note 169.

[217] *Final Report*, NAT'L SEC. COMM'N ON A.I. at 227 (Mar. 2021), https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf.

Not only are companies unsure of what export control system they are under for export controls but bringing this regime into the CFIUS mandatory declaration adds more confusion. Even with all the uncertainty surrounding "critical technologies," no mandatory review is required unless U.S. export authorization is required to export the critical technologies. This is unclear for companies as the export system is complex, and it is not required for companies to know what U.S. export authorization they need. Furthermore, many U.S. companies do not export and would not be subject to any export laws. There are no requirements for these companies to understand or be involved with the complex export controls system. For such an important protection from nefarious foreign investments, CFIUS is failing to review transactions that it should because of the uncertainty in its requirements for mandatory filings.

The uncertainties in the review process and the reliance on companies to voluntarily file have deleterious effects on the U.S.'s race to control the 5G market and to control the data acquired from wearable technology. Whoever wins the race will set the standard for 5G, which will include the country's technology. If China wins and sets a standard using Chinese equipment, the Chinese government will have direct access to the data of all users.[218] China's surveillance scheme opens the door to viewing an American citizen's everyday life. The amount of information vulnerable to China is astounding. Using 5G technologies from Chinese or other foreign untrusted companies can expose data to "malicious software and hardware, counterfeit components, and component flaws…" and "could increase the risk of compromise to the confidentiality, integrity, and availability of network assets."[219] Data can be intercepted, manipulated, disrupted, and destroyed, leading to more chances for attack and greater vulnerability.[220] From a simple Fit Bit watch to personal assistant eye contacts, foreign countries may launch new attacks on the personal freedoms and security of the U.S.

B. Practical Problem Analysis: Companies Can Easily Circumvent CFIUS Review

These deficiencies in the CFIUS review cause foreign investment to grow without protection from the risks to data privacy and national security. 5G wearable technology is upon us and will grow exponentially into the future. Wearable technology and other sensitive technologies spurred by 5G need protection from foreign investment. This is especially a problem

---

[218] GALLAGHER & DEVINE, *supra* note 4, at 8; *see* INSA Cyber Council, *supra* note 16; *see also* Arjun Kharpal, *Huawei Says It Would Never Hand Data to China's Government. Experts Say It Wouldn't Have A Choice,* CNBC (Mar. 4, 2019), https://www.cnbc.com/2019/03/05/huawei-would-have-to-give-data-to-china-government-if-asked-experts.html.

[219] Cybersecurity and Infrastructure Agency, *supra* note 74.

[220] *Id*.

because of how much information is vulnerable to China when Chinese investors gain access to data gathered through wearable technology – like eye contact lenses.[221]

A company can circumvent CFIUS review by identifying itself as not subject to U.S. export authorization. For example, a U.S. eye contact lenses company may launch a research and development team to create personal assistant eye-contacts. Imagine this R&D team successfully develops the personal assistant contacts and decides to merge with a Chinese company. It wants to merge to get the investment benefits that the Chinese company will provide. The Chinese company invests and gets, say, 9% of control.

Under the current CFIUS-FIRRMA requirements, the contact lenses company does not fall under any mandatory review as it does not fall under the "critical technologies" definition that relies on whether U.S. export authorization is required; and there is no voting interest of 25% or more.[222] It could fall under voluntary review, which is entirely at the company's discretion.[223] The contact lenses company finishes the transaction without CFIUS review, and now China can access the company's R&D.[224] China may use these eye-contact personal assistants as surveillance on individual Americans. It can collect information from anyone who uses this new wearable technology and can use the data for harmful purposes.[225] Moreover, if an individual, using the eye-contacts, works on U.S. government projects, the Chinese government can see everything the individual does. As illustrated, the amount of data collected is profound, and the amount of sensitive and potential national security concerns is even more astounding. The concern is that China would have access to data which they can use against individuals and the U.S. – whether through stealing intellectual property, launching cyberattacks, or bringing more risks to national security and privacy.

A company that receives 90% of its revenue from optical lens manufacturing and 10% from developing eye-contact personal assistants would not be required to file for mandatory review under FIRRMA.[226] Suppose the Chinese invested in this company under the 25% voting interest,

---

[221] *See* Kharpal, *supra* note 218.

[222] 31 C.F.R. §§ 800.215, 800.401 (2020).

[223] 31 C.F.R. § 800.402 (2020).

[224] "Stakeholder inclusion [in Research and Development] does not necessarily follow a pattern and may vary according to the nature and flow of information between those responsible for the exercises and the participants." Luciana Maines da Silvia et al., *The Role of Stakeholders in the Context of Responsible Innovation: A Meta-Synthesis*, MPDI, at 6 (Mar. 23, 2019). Each company's decision to include stakeholders in the R&D will vary, but the risks to national security and data privacy are too high to assume stakeholders never or rarely have access to this information. *See id.*

[225] Foreign Investment Risk Review Modernization Act of 2018, H.R. 5841 §§ 201(3)(B)(II)(aa), 308(13), 115th Cong. § 201 (2018).

[226] *See* 31 C.F.R. §§ 800.224, 800.301 (2020).

then the company is not required to file a notice to CFIUS or undertake a mandatory review. China would have access to the eye-contact personal assistant and the mass of private data they collect.

C. A Solution to Strengthen CFIUS's Review by Requiring More Mandatory Filings and Redefining "Critical Technologies"

CFIUS must provide a bright line for mandatory filing requirements and strengthen the export control definition for critical technologies. Congress must work to understand that success for the Race to 5G and wearable technology privacy and data concerns will depend on the level of clarity around export controls that has not been seen in the past. CFIUS should also focus on foreign investment from specific countries. For example, CFIUS could require a mandatory review based on any Chinese investment or investments from other countries of concern. This would provide CFIUS an opportunity to review transactions before they occur and before Chinese investors have access to critical technologies. While this may seem overly broad, as not all Chinese investment may give national security concerns, this solution provides notice to the world that the U.S. is acting offensively.

Congress should amend FIRRMA to provide for mandatory review of transactions that are not based on businesses' self-identified export control system and bright-line mandatory filing requirements that are not tied to vague descriptions of investor accessed data information. Export administration regulations should expand to control information and technology that is sensitive or relevant to the national security of the U.S. This should include identifying information and other data about Americans regulated at the state level and in many countries under data privacy laws. Enforcement resources and penalties, as well as the administration's willingness to enforce the laws, are also an area where improvement will be necessary to promote compliance. Additionally, for a more specific review, CFIUS could require foreign investments from specific countries to be reviewed, but this preferential policy may cause backlash from the countries. CFIUS could also require enhanced disclosure for investors from specific countries.

The benefits of this solution include an increase in national security protections and an increase in American individuals' privacy protections. It will allow a greater review of the transactions that may harm these concerns and will give notice to the companies on what the FIRRMA terms mean. The solution will increase the U.S.'s hold on 5G technology as it will not open doors to Chinese equipment and control in the U.S. market. As such, it will benefit the U.S. in the Race to 5G and future races to innovative technologies.

Redefining CFIUS has both benefits and shortcomings. The solution avoids the practical problem. The company can avoid CFIUS review because of the uncertainty in the export control definition. For example, a company

could identify its optical lens R&D under developing critical technologies as well as its primary contact lens operations. Because national security will be more broadly defined, to concern anything which may grant significant surveillance opportunities, CFIUS will review the transaction before it happens. Additionally, CFIUS could require that China's investment in this technology be limited to monetary funds and returns, not access to the personal data collected.

Academic scholars also point out some significant problems with CFIUS like that there is no definition of national security, no monetary threshold of reviewable transactions available, and only a broad definition of "control."[227] The broad terms provide discretion for CFIUS review, but they also provide room for companies to avoid filing mandatory reviews. A stronger, more defined set of terms would provide more notice and an aggressive approach to foreign investment.

The detriments to this solution are the costs of implementing an aggressive law to protect the U.S. The CFIUS review committee would need to grow to be able to handle the massive amount of review it will need to conduct. Companies may be unhappy that they cannot do mergers and acquisitions with foreign countries without review. However, without requiring review, the risks to the U.S.'s national security are too high.

Another possible detriment is stifling innovation. Foreign investment helps spur innovation. Adding more review before foreign investment and transactions occur may hurt the free market by imposing more costs. There must be a balance between securing data privacy and national security and supporting innovation to win the 5G race. This balance is difficult to find in practice, but the risks of not securing them are too high. This solution to provide a stronger CFIUS review would be a first step to finding that balance.

While this solution may be a first step, there are other alternatives that the U.S. may consider implementing.

D. Alternatives

This comment will examine the alternative solutions by discussing U.S.-based alternatives, then international-based alternatives. These alternatives may be considered instead of strengthening the CFIUS review or in tandem with it. This comment suggests the best solution is to strengthen the CFIUS review in tandem with the U.S. government's increased investment in 5G wearable technology and with a focus on working with allies to have a unified front against threats to data privacy and national security.

---

[227] *See* 31 C.F.R. § 800.208 (2020).

i. U.S.-Based Alternatives

The U.S.-based alternatives include using a laissez-faire approach which would continue the status quo, increasing U.S. investment, implementing stricter requirements, and using state law to combat threats to data privacy and national security.

a. Laissez-Faire Approach

Instead of creating a stronger legal system to deal with national security concerns, the U.S. can continue to act defensively against Chinese involvement. Scholars argue that dealing with concerns as they develop is a better method of regulation because it allows for innovation without suffocation.[228] By using the legal systems in place already and keeping the status quo, the U.S. would allow wearable technologies to grow with little limitations. Too much limitation on wearable technologies at an early stage of their development could be premature and too rigid, which could stifle innovation.[229] Allowing time for 5G wearable technology to grow would give time for societal and individual adaptations to adjust to wearable technologies.[230] As these technologies mature, regulation can be introduced in the future when we know more about the threats in place. Legal systems already in place, like various common laws, can provide legal recourse for individuals who have privacy invasions.[231] However, this alternative would be inadequate to protect from the current threats to 5G wearable technology. As technology grows, so does the threat to data privacy and national security. These threats as they are now are not adequately addressed through the CFIUS review process. The current process is too voluntary and uncertain for companies. Continuing this process as is will continue the threat. This alternative would provide too much weight to innovation without enough protection for data privacy and national security.

Relying on the legal systems in place is inadequate because it is too retroactive and uncertain. The FTC has brought enforcement actions against companies to protect American privacy and data security.[232] However, the FTC is just enforcing the privacy from U.S. companies using this data in unclear ways; it is not protecting the Chinese threat to privacy concerns. Additionally, using legal systems in place is problematic as it is difficult to pinpoint where Chinese surveillance is occurring, what entity is surveilling, and what damages occurred because of privacy breaches.

---

[228] *See* Thierer, *supra* note 12, at 52.
[229] *See id.* at 47.
[230] *See id.* at 78-79.
[231] *See id.* at 102-03.
[232] *See id.* at 106.

Accordingly, a laissez-faire approach is not an adequate alternative because it does not protect from threats to data privacy and national security proactively.

b. Investing

Instead of strengthening CFIUS, the U.S. could instead invest in wearable technology and other innovations itself. The federal government could create policies to promote innovation, protect national security in wearable technology, and provide incentives for domestic research and development. While this alternative may be helpful to boost innovation, it may not have enough power to block foreign investment, thus posing a risk to national security. This alternative would not stop any Chinese threat to investments in 5G wearable technology. However, this alternative for the U.S. to increase its investment and policies to promote 5G wearable technology, used in tandem with a stronger CFIUS, may provide the right kind of balance needed between innovation and national security.

c. Increasing Restrictions

Congress could grant CFIUS more authority to implement restrictions on banning U.S. investment in Chinese strategic firms, like tech companies.[233] CFIUS could apply a presumption of denial from Chinese investment companies in key sectors. Instead of clarifying and strengthening the mandatory review, having a presumption of denial would increase the burden of a CFIUS review and could chill Chinese investment. This presumption would increase certainty in that most Chinese investment would be blocked. However, it would not consider the benefits that Chinese investment can bring to innovation and might cause more harm by creating a bias against specific countries. Accordingly, a presumption of denial may not be the best solution.

d. State Law Approach

State corporation law guidelines developed in lower courts can augment CFIUS's policy interests.[234] Instead of relying on CFIUS, state laws could implement protections against hostile takeovers from foreign companies to avoid Chinese companies manipulating board officers and their decisions to have favorable Chinese policies in place. While the benefit of a state law approach would allow for state experimentation, it would take years for there to be a uniform approach that protects the nation.

[233] COTTON, *supra* note 92, at 31.
[234] *See* Westbrook, *supra* note 25, at 646.

ii. International-Based Alternatives

Instead of focusing on U.S. based alternatives, the U.S. could work on an international front to combat threats to data privacy and national security from 5G wearable technology. This section will first discuss how the U.S. could work with allies, then discuss opening a dialogue with China.

a. Working with Allies

In the alternative to reforming CFIUS, the U.S. could try to mitigate the risks from the Chinese threat by working with its allies to promote data privacy in 5G wearable technology. Encouraging democratic values and secure networks with our allies would allow a comprehensive front against threats to our national security.[235] With countries "standing" together as a unified body to thwart threats, the U.S. could encourage a reduced dependency on foreign, especially Chinese, technologies. The U.S. and its allies could also work to "build more resilient supply chains[] and develop technology standards and norms that reflect democratic values."[236] The U.S. has participated in this approach with the Prague Proposals[237] which are "recommendations for nations to consider as they design, construct and administer their 5G (fifth-generation) telecom infrastructure."[238] The Prague Proposals arose from the Czech Republic's Prague 5G Security Conference.[239] Government officials from thirty-two countries, the European Union, and NATO participated in this conference to open discussion and provide recommendations for cybersecurity frameworks.[240] While opening this discussion between countries is a great first step, there needs to be more action.[241]

b. Establish a Dialogue with China

Instead of strengthening CFIUS's review towards Chinese investment, the U.S. could establish a diplomatic dialogue with China.[242] Opening this dialogue between the countries about innovations like 5G

---

[235] National Security Commission on Artificial Intelligence, *Final Report*, at 2, 6, https://www.nscai.gov/wp-content/uploads/2021/03/Full-Report-Digital-1.pdf (last visited Apr. 16, 2021) [hereinafter Final Report].

[236] *Id.* at 163.

[237] *Prague 5G Security Conference Announced Series of Recommendations: The Prague Proposals*, GOV. CZECH (Mar. 5, 2019), https://www.vlada.cz/en/media-centrum/aktualne/prague-5g-security-conference-announced-series-of-recommendations-the-prague-proposals-173422/.

[238] Leigh Hartman, *Countries Agree On 5G Security in Prague*, SHARE AMERICA (Mar. 13, 2019), https://share.america.gov/countries-agree-on-5g-security-in-prague/.

[239] *Id.*

[240] *Id.*

[241] *Id.*

[242] Final Report, *supra* note 235, at 167.

wearable technology would set a light on the threats to data privacy and national security and help mitigate them through discussions about our concerns. Building a stronger relationship with China would benefit the U.S. in terms of 5G wearable technology because foreign investments would not be stifled in any, but there would be more transparency with our concerns that the Chinese could address. As this is a very political alternative, many factors would play into whether this dialogue could be successful. Both the U.S. Administration and the Chinese government would need to be willing to work together. Accordingly, this alternative would be better paired with the solution to strengthen the CFIUS review.

This comment's solution is better than the status quo because it provides more protection for American citizens, especially with the vast risks 5G wearable technology brings to privacy. The other alternatives, collectively, do not assess the issue with the export control definitions. There is a lack of literature discussing the new scheme. More research should be done to innovate a new classification system for companies.

IV. CONCLUSION

When you take your eye contact lenses out at the end of the day, you do not want to be afraid of who saw, heard, and experienced everything you did. In the Race to 5G, protecting data privacy and national security in wearable technology is extremely important to win the race and mitigate the risks from foreign investment. CFIUS's review process is not adequately protecting from these risks because of the voluntariness of filing declarations, the basis of which is on a company's self-classification, and uncertainty arising from the definition of "critical technology" based on an outdated export controls system.

Congress should amend FIRRMA to provide for mandatory reviews of transactions that are not based on an export control regulatory scheme that is historically known for its uncertainty and provide bright-line mandatory filing requirements that are not tied to vague descriptions of investor accessed data information. Export administration regulations should be expanded to control information and technology that is sensitive or relevant to the national security of the U.S., including identifying information and other information about Americans regulated at the state level and in many countries under data privacy laws. Enforcement resources and penalties, as well as the administration's willingness to enforce the laws, is also an area where improvement will be necessary to promote compliance.

Reviewing the export control "critical technologies" definitions and requiring mandatory review in more cases will provide greater CFIUS power over Chinese investment. In the race to 5G, the U.S. needs aggressive laws to protect its control of technology over foreign countries. This comment's

solution will provide an opportunity for winning the 5G race and future races, too.

THE VEXING CONTRADICTION OF U.S. JURISDICTION OVER EMBASSY PROPERTY IN THE CRIMINAL VERSUS CIVIL CONTEXTS

Samantha E. Lewis[1]

I. INTRODUCTION

Picture this: you are a foreign service officer on mission in Port-au-Prince, Haiti. The United States Department of State has stationed you and your spouse in a government-leased house within the U.S. Embassy property. According to what you have been told, the house is "earthquake proof," and in the event of an earthquake you will be safest by staying in the house. Despite the well-known fact that Haiti is no stranger to earthquakes, you feel assured that the house you will be living in for the foreseeable future is safe.

Unsurprisingly, an earthquake strikes, and it is devastating. Remembering what you were told, you and your spouse take shelter in the house. Before you realize what is happening, the house that is supposed to be "earthquake proof" is crumbling down around you. You and your spouse are trapped, and it is too late to get out of the house. The next thing you know, you are in a hospital somewhere in Haiti. You find out that your leg was crushed under the rubble, and you will likely lose it due to the severity of your injuries—but sadly, that is not all. Your spouse was trapped under the house for days and suffered a traumatic brain injury as a result. Your spouse is now paralyzed and will never be the same.

Obviously, the State Department-supplied housing that was supposed to be "earthquake proof" was the furthest thing from. After all, there was practically nothing left of the house after the earthquake. You and your spouse cannot go back to work due to the severity of your injuries, and you will both need very expensive and extensive medical care. You will need a prosthetic leg, and your spouse will need constant, around-the-clock, lifelong care, all of which will be outrageously expensive. How will you afford this, considering you will not be able to go back to work? You start thinking of compensation — who can you look to for damages? Your most obvious choice is the United States government since it was your employer, it supplied you the "earthquake proof" house, and because of its negligence and misrepresentation, your life will never be the same.

You decide to seek the advice of counsel and file a complaint in federal district court in accordance with the Federal Tort Claims Act

[1] Juris Doctor, George Mason University Antonin Scalia Law School. With many thanks and gratitude for the support of my friends, family, and the entire ILJ editorial team. Special thanks to my husband, Brandon Lewis, my parents, Sandra and Philip McCurry, and my mentor, Alison Mullins, for their continued support.

("FTCA"), the act that allows private parties to sue the federal government.[2] To your surprise, your complaint gets dismissed. Why? According to the Court, it is simple—the FTCA has a codicil called the "foreign country exception," which bars any claims "arising out of a foreign country."[3] This just does not seem right, so you exhaust all of your appeals.[4] Nevertheless, you are left with no other options — you cannot recover from the federal government, meaning you cannot recover at all.[5]

Would it surprise you to learn that the situation described above in fact *is* the current state of the law? I am sure you are thinking, "but how can this be fair?" Unfortunately, it is the current state of the law, at least according to some of the federal circuit courts and many district courts.[6] The above narrative is based on the real case, *Kathy-Lee Galvin & Blaise Pellegrin v. United States*.[7] Kathy-Lee and her husband, Blaise, are real people, and they were *not* able to recover *anything*, despite being employees of the United States Department of State, living in housing supplied to them by the Department of State advertised to them as "earthquake proof", and despite their catastrophic injuries.[8]

At first glance, this seems like a straightforward application of the law—embassy property is *technically* on foreign territory, and if the claim arose in a foreign country, then it is barred.[9] The circuit courts have indeed approached these claims in this basic and formulaic way.[10] Nevertheless, although it appears simple, there are multiple layers and caveats that make this particular exception far more complex.

---

[2] 28 U.S.C. § 2674 (1948) ("The United States shall be liable, respecting the provisions of this title relating to tort claims, in the same manner and to the same extent as a private individual under like circumstances, but shall not be liable for interest prior to judgment or for punitive damages.").

[3] 28 U.S.C. § 2680(k) (2018).

[4] Galvin v. United States, 859 F.3d 71 (D.C. Cir. 2017), *cert. denied*, 138 S. Ct. 456 (2017).

[5] This narrative is based on the case of *Galvin v. United States,* 859 F.3d 71. I worked on the Supreme Court petition for this case when I was a paralegal at the firm that represented her and her husband.

[6] *See, e.g.*, Macharia v. United States, 334 F.3d 61, 69 (D.C. Cir. 2003) (holding the FTCA's sovereign immunity waiver does not extend to acts or omissions arising in territory subject to the sovereign authority of another nation because of the foreign country exception); Meredith v. United States, 330 F.2d 9, 10 (9th Cir. 1964) (holding the acts and omissions upon which appellant based her action occurred in Bangkok, Thailand, so the suit was barred by the foreign country exception); Romero v. Consulate of U.S., 860 F. Supp. 319, 324 (E.D. Va. 1994) (dismissing claims by aliens under the FTCA alleging emotional distress caused by the negligent denial of visas for entry to the U.S. by consular officials in Colombia because claims were barred by the foreign country exception to the FTCA); Gerritson v. Vance, 488 F. Supp. 267, 268-70 (D. Mass. 1980) (granting the U.S.'s motion to dismiss a suit under the FTCA, holding that the plaintiff's claim, which arose from an incident on the grounds of the Embassy in Zambia, occurred in a foreign country within the meaning of the foreign country exception).

[7] *Galvin*, 859 F.3d at 71.

[8] *Id.*

[9] *See* 28 U.S.C. § 2680(k) (2018).

[10] *See, e.g., Galvin*, 859 F.3d at 71; *Macharia*, 334 F.3d at 69; *Meredith*, 330 F.2d at 9.

What makes this situation more vexing is that there exists a conflicting statute aimed at criminal activity on embassy property, which was enacted around the same time as the FTCA's foreign country exception.[11] This statute seemingly gives the United States jurisdiction in the criminal context in the exact area that the foreign country exception purports to cut off jurisdiction in the civil context.[12] Why is it that Kathy-Lee could be prosecuted according to United States law, under United States jurisdiction, in a United States Federal Court if she *murdered* her husband in the embassy housing, but she *cannot* recover damages according to United States law, under United States Jurisdiction, in a United States Federal Court after being crushed under housing supplied to her *by the United States*? It is this contradiction and double standard that I hope to explore further in this Comment.

Part II of this Comment will explore the background of the two statues, starting with the foreign country exception, then the special maritime and territorial jurisdiction defined in 18 U.S.C. § 7. Part II will also discuss Supreme Court and Circuit Court decisions addressing each statute.

Part III will then analyze the practical and legal implications of this apparent statutory contradiction and propose solutions to these problems. One solution requires amending the foreign country exception so that it is clear about what the exception encompasses, explicitly stating that the property procured for an embassy is not subject to the exception. Another solution, although perhaps more cumbersome, requires the Supreme Court to grant certiorari to a case and create a rule construing the foreign country exception in a way that would exclude embassy property from its reach, just as it has done with the jurisdiction conferred through 18 U.S.C. § 7(3).[13]

These solutions can find support in the statute defining special maritime and territorial jurisdiction, especially since it was enacted around the same time as the foreign country exception, and courts, including the Supreme Court, have examined it explicitly in the embassy context.[14]

II. BACKGROUND

It is important to first discuss both the FTCA's Foreign Country Exception and the Special Maritime and Territorial Jurisdiction of the United States, their purposes, their legislative histories, and cases discussing each statute. This discussion will provide important context and understanding for the subsequent analysis.

---

[11] *See* 18 U.S.C. § 7(3) (2018).

[12] *See id.*; United States v. Erdos, 474 F.2d 157, 160 (4th Cir. 1973) (holding that the district court had jurisdiction to try an American citizen for a crime occurring within the American Embassy located in a foreign country).

[13] *See, e.g.*, United States v. Corey, 232 F.3d 1166 (9th Cir. 2000); *Erdos*, 474 F.2d at 157.

[14] *See, e.g.*, *id.*

A. A Basic Overview of The Federal Tort Claims Act

Prior to the enactment of the FTCA, the United States could not be sued under the doctrine of sovereign immunity.[15] Sovereign immunity is defined as a "government's immunity from being sued in its own courts without its consent" and a "state's immunity from being sued in federal court by the state's own citizens."[16] In *Kawananakoa v. Polyblank*, Justice Holmes said that the doctrine of sovereign immunity derives from "the logical and practical ground that there can be no legal right as against the authority that makes the law on which the right depends."[17] The FTCA basically suspends the United States' sovereign immunity in tort actions caused by the acts and omissions of government officials and employees.[18] The act makes it so the government can be held liable for torts the same way a private citizen could be.[19]

Several exceptions to the FTCA are listed in section 2680.[20] The foreign country exception is contained in Section 2680(k), and says that the United States shall not be liable for "[a]ny claim arising in a foreign country."[21] Although the term "foreign country" has been litigated in cases and discussed in secondary materials, it is not defined elsewhere in the FTCA.[22]

B. Legislative History of the Federal Tort Claims Act

After twenty-eight years of drafting and redrafting, as Justice Reed says, "Congress was ready to lay aside a great portion of the sovereign's ancient and unquestioned immunity from suit," and finally enacted the FTCA.[23] The "Federal Tort Claims Act" was the official short title passed by the Seventy-Ninth Congress on August 2, 1946, as Title IV of the Legislative

---

[15] *See* United States v. Spelar, 338 U.S. 217, 220 (1949).

[16] *Sovereign Immunity,* BLACK'S LAW DICTIONARY (10th ed. 2014).

[17] Kawananakoa v. Polyblank, 205 U.S. 349, 353 (1907).

[18] *See* 28 U.S.C. §§ 1346(b), 2671-80 (2018).

[19] 28 U.S.C. §1346(b) (2018) (excluding interest prior to judgment or punitive damages).

[20] 28 U.S.C. § 2860(a)-(n) (2018). For example, the act provides for exceptions for claims such as those that arise "out of the loss, miscarriage, or negligent transmission of letters or postal matter" (b), "for damages caused by the imposition or establishment of a quarantine by the United States" (f), and "from the activities of the Tennessee Valley Authority"(l). *Id.*

[21] 28 U.S.C. § 2860(k) (2018). This exception is commonly referred to as the "foreign country exception" and will be referred to as such throughout this discussion.

[22] *See, e.g.*, Galvin v. United States, 859 F.3d 71 (D.C. Cir. 2017); 158 A.L.R. Fed. 137 (Originally published in 1999).

[23] United States v. Spelar, 338 U.S. 217, 221 (1949).

Reorganization Act.[24] Title IV was substantially repealed and reenacted as sections 1346 and 2671 on June 25, 1948.[25]

The foreign country exception has been part of the FTCA since its first enactment in 1942.[26] Originally, the exception read, "arising in a foreign country *on behalf of an alien*," making the government's liability turn on the injured party's citizenship, but that part was excised from the exception before the final version was enacted.[27] An often cited and notable dialogue between Assistant Attorney General Francis Shea and Congressman Robinson of the House Judiciary Committee is illustrative in showing what Congress may have intended in including the foreign country exception. The dialogue reads as follows:

> **MR. SHEA** ... Claims arising in a foreign country have been exempted from
> this bill, H.R. 6463, whether or not the claimant is an alien. Since liability is
> to be determined by the law of the situs of the wrongful act or omission it is
> wise to restrict the bill to claims arising in this country. This seems desirable
> because the law of the particular State is being applied. Otherwise, it will lead
> I think to a good deal of difficulty.
> **MR. ROBSION**. You mean by that any representative of the United States
> who committed a tort in England or some other country could not be reached
> under this?
> **MR. SHEA**. That is right. That would have to come to the Committee on
> Claims in the Congress.[28]

It is clear from this history that Congress was concerned about opening up the United States to liability under the laws of other countries.[29] Nonetheless, it is also clear from the Congressional statement of purpose that "fair play and justice" was a primary goal of Congress in adopting the FTCA.[30]

---

[24] 28 U.S.C. § 2671 (2018); Legal Information Institute Online, *Definitions*, CORNELL UNIV. L. SCH., https://www.law.cornell.edu/uscode/text/28/2671 (last visited Apr. 16, 2021).

[25] *Id.* Coincidentally, the statute authorizing Special Maritime and Territorial Jurisdiction, discussed later, was also part of the Legislative Reorganization Act of 1948.

[26] *Spelar*, 338 U.S. at 219-21.

[27] H.R. 5373, 77th Cong., 2d Sess., § 303 (12).

[28] *Spelar*, 338 U.S. at 221; *See also* Mark Dean, Smith v. United States*: Justice Denied under the FTCA Foreign Country Exception*, 38 ST. LOUIS U. L.J. 553, 561 (1993).

[29] *Spelar*, 338 U.S. at 221.

[30] COMMITTEE ON THE OFFICE OF ATTORNEY GENERAL, NATIONAL ASSOCIATION OF ATTORNEYS GENERAL, SOVEREIGN IMMUNITY: THE TORT LIABILITY OF GOVERNMENT AND ITS OFFICIALS (1979). The first statement of purpose reads: "A desire on the part of the federal

Certainly, barring any and all claims by people like Kathy-Lee Galvin explicitly goes against Congress's policy goal in enacting the FTCA.

Furthermore, the legislative history does not provide a clear indication as to what the foreign country exception is specifically intended to cover.[31] It was originally proposed that the FTCA would *only* cover the United States, Puerto Rico, and the Canal Zone, but Congress ultimately decided against providing specific geographical areas covered under the foreign country exception.[32]

Rejection of the geographical and citizenship requirements left the scope of the exception inconclusive and subject to interpretation.[33] As Mark Dean explains, "the implication is that since the drafters rejected a proposal that would have specifically limited the Act to defined areas, the purpose of the exception was only to avoid United States liability under foreign law," not to leave the government free from all liability.[34] Federal Courts on all levels have attempted to interpret the foreign country exception, but the pursuit to explicitly define the phrase "foreign country" has been less than successful.[35]

C. "Foreign Country" Defined Elsewhere in the United States Code and Case Law

The phrase "foreign country" appears more than 2,000 times when searched on Westlaw.[36] Yet defining "foreign country" with exact specificity has proven to be difficult. The Supreme Court addressed the difficulty in defining "foreign country" in *Burnet v. Chicago Portrait Co.* In *Burnet*, the Court said:

> The word "country" in the expression "foreign country," is ambiguous. It may be taken to mean foreign territory or foreign government. In the sense of territory, it may embrace all the territory subject to foreign sovereign

government in the interests of justice and fair play to permit a private litigant to satisfy his legal claims for injury or damage suffered at the hands of the United States employee acting in the scope of his employment." *Id.*

[31] Dean, *supra* note 28, at 560.

[32] *Tort Claims Against the United States: Hearings on S. 2690 Before the Subcomm. of the Senate Comm. on the Judiciary*, 76th Cong., 3d Sess., at 65 (1940).

[33] Dean, *supra* note 28, at 562.

[34] *Id.*

[35] *See, e.g.*, Sosa v. Alvarez-Machain, 542 U.S. 692, 692 (2004); Galvin v. United States, 859 F.3d 71, 73 (D.C. Cir. 2017); Meredith v. United States, 330 F.2d 9, 10 (D.C. Cir. 2017).

[36] *See, e.g.*, 26 U.S.C. § 896 (2018) (Adjustment of tax on nationals, residents, and corporations of certain foreign countries); 19 U.S.C. § 2905 (2018) (Accession of state trading regimes to General Agreement on Tariffs and Trade or WTO); 19 U.S.C. § 2906 (2018) (Definitions); 19 U.S.C. § 3103 (2018) (Investigation of foreign telecommunications trade barriers); 42 U.S.C. § 2077(a) (2018) (Interagency review of applications for the transfer of United States civil nuclear technology).

> power. When referring more particularly to a foreign government, it may describe a foreign state in the international sense… or it may mean a foreign government which has authority over a particular area or subject matter… the sense in which it is used in a statute must be determined by reference to the purpose of the particular legislation.[37]

The term "foreign country" as applied to the foreign country exception to the FTCA is not defined in the Act's definitions section,[38] so it is not clear what exactly the exception is referring to. The United States Code is not replete with any definition of "foreign country" in any context. Title 19, Chapter 17 of the United States Code does provide one definition for "foreign country."[39] This chapter says, "[t]he term 'foreign country' includes any foreign instrumentality.[40] Any territory or possession of a foreign country that is administered separately for customs purposes, shall be treated as a separate foreign country."[41]

In *United States v. Spelar*, discussed in greater detail later, the Supreme Court tried to define "foreign country" for the purposes of the foreign country exception in a straightforward and simplistic way.[42] The Court said there is "no more accurate phrase in the common English usage than 'foreign country' to denote territory subject to the sovereignty of another nation."[43] This definition, however, forms a rather circular argument: a "because we say so" kind of approach. Justice Frankfurter's concurrence alludes to the circularity of this definition:

> To assume that terms like 'foreign country' and 'possessions' are self-defining, not at all involving a choice of judicial judgment, is mechanical jurisprudence at its best. These terms do not have fixed and inclusive meanings, as is true of mathematical and other scientific terms. Both 'possessions' an[d] 'foreign country' have penumbral meanings, which is not true, for instance, of the verbal designations for weights and measures. It is this precision of content which differentiates scientific from most political, legislative and legal language.[44]

---

[37] Burnet v. Chicago Portrait Co., 285 U.S. 1, 5-6 (1932). *Burnet* discussed the ambiguity in "foreign country" in reference to the Revenue Code.

[38] 28 U.S.C. § 2671 (2000). This section does define a "federal agency" and an "employee of the government," but provides no other definitions.

[39] 19 U.S.C. § 2906(2) (2018).

[40] *Id.*

[41] *Id.*

[42] United States v. Spelar, 338 U.S. 217, 219 (1949).

[43] *Id.*

[44] *Id.* at 223 (Frankfurter, J., concurring).

As courts have approached other cases involving the foreign country exception, they continue to cite the "because we say so" style of defining "foreign country" for the purposes of the foreign country exception.[45] The problem with this definition, as Justice Frankfurter points out, is that there is no specificity to it. For example, what happens when a territory is subject to the dual sovereignty of two different nations? An Air Force base is arguably under the sovereignty of the United States, even if it is technically situated in another country.[46] This *was* the argument in *Spelar*, which the Court rejected, but without really explaining why this argument had been rejected.[47]

D. The Current State of the Case Law: United States v. Spelar, Sosa v. Alvarez-Machain, and Meredith v. United States

As the three cases discussed below make clear, to argue that the term "foreign country" does *not* include embassy property is contrary to the current state of the law. There have been many lower circuit court and district court decisions that explicitly hold that claims arising on embassy property are barred by the foreign country exception.[48] Nonetheless, none of these cases entirely foreclose the possibility of allowing these kinds of claims.

i. *United States v. Spelar*

United States v. Spelar is the most important and most cited case involving the foreign country exception.[49] Lillian Spelar, as Administratrix of the Estate of her husband Mark Spelar, sued the United States under the FTCA for Mark's death in an airplane crash at Harmon Field, Newfoundland, an air base leased for 99 years by Great Britain to the United States.[50] Lillian Spelar alleged that the fatal accident was caused by the government's negligent operation of Harmon Field and sought damages under Newfoundland's wrongful death statute.[51] The district court held that the claim was barred by the foreign country exception and dismissed the complaint for lack of jurisdiction, but the Court of Appeals reversed.[52] The Supreme Court reversed the decision of the Court of Appeals, holding that the Newfoundland air base fell within the foreign country exception.[53]

---

[45] *See, e.g.*, Sosa v. Alvarez-Machain, 542 U.S. 692, 694 (2004); Galvin v. United States, 859 F.3d 71 (D.C. Cir. 2017); Meredith v. United States, 330 F.2d 9 (9th Cir. 1964).

[46] *See Spelar*, 338 U.S. at 218-19.

[47] *Id.* at 219.

[48] *See, e.g.*, *Sosa*, 542 U.S. at 692; *Galvin*, 859 F.3d at 73; *Meredith*, 330 F.2d at 10.

[49] *See, e.g.*, *Sosa*, 542 U.S. at 707; Dean, *supra* note 28, at 553; Kelly McCracken, *Away from Justice and Fairness: The Foreign Country Exception to the Federal Tort Claims Act*, 22 LOY. L.A. L. REV. 603, 604 (1989).

[50] *Spelar*, 338 U.S. at 218.

[51] *Id.*

[52] *Id.* at 218-19.

[53] *Id.* at 222.

The Supreme Court based its decision in part on the legislative history and in part on the words of the exception on its face without further analysis into any possible ambiguities.[54] The Court held that "[s]ufficient basis for our conclusion lies in the express words of the statute"[55] because the 99-year lease between Great Britain and the United States "did not and [was] not intended to transfer sovereignty over the leased areas from Great Britain to the United States."[56] Because the Air Force base where Mr. Spelar's death occurred "remained subject to the sovereignty of Great Britain," the claim arose in a foreign country and was thus barred.[57]

Ms. Spelar's claim may have been more successful had she sued according to United States' wrongful death laws, but the Court did not discuss that possibility.[58] Nonetheless, many courts, including the Supreme Court in *Sosa v. Alvarez-Machain*, have cited to this reasoning in denying subsequent claims pursuant to the foreign country exception.[59]

Justice Frankfurter and Justice Jackson submitted concurring opinions.[60] Justice Frankfurter, although he agreed that the claim was barred by the foreign country exception, argued that "a 'foreign country' in which the United States has no territorial control does not bear the same relation to the United States as a 'foreign country' in which the United States does have the territorial control that it has in the air base in Newfoundland."[61] Justice Jackson reached the same result, but did not agree with the majority's analysis.[62] He argued, much like embassies in this context, that Congress had treated U.S air bases differently in two different pieces of legislation, leading to confusion.[63] He explained "[t]o those uninitiated in modern methods of statutory construction it may seem a somewhat esoteric doctrine that the same place at the same time may legally be both a possession of the United States and a foreign country."[64]

---

[54] *Id*. at 219-21.
[55] *Id.* at 219.
[56] *Id.*
[57] *Id.*
[58] There are, of course, choice of law issues that would need to be explored here. Nonetheless, that is a topic that could be the subject of an entire comment and will not be discussed in depth here.
[59] *See, e.g*., Sosa v. Alvarez-Machain, 542 U.S. 692 (2004); Meredith v. United States, 330 F.2d 9, 10-11 (9th Cir. 1964); Hourani v. Mirtchev, 796 F.3d 1, 5 (D.C. Cir. 2015); Gerritson v. Vance, 488 F. Supp. 267, 268 (D. Mass. 1980).
[60] *Spelar*, 338 U.S. at 222-25.
[61] *Id.* at 223.
[62] *Id.* at 224.
[63] *Id.* at 225.
[64] *Id.*

ii. *Sosa v. Alvarez-Machain*

In *Sosa*, the plaintiff, a Mexican national, was acquitted of murder after facing prosecution in the United States.[65] The plaintiff claimed that he was abducted and transported to the United States to face prosecution, and sought damages from the United States for false arrest under the FTCA.[66] The district court granted the government's motion to dismiss the FTCA claim, but awarded summary judgment and damages for a claim pursuant to the Alien Tort Statute.[67] The circuit court affirmed the Alien Tort Statute judgment, but reversed the dismissal of the FTCA claim.[68] The Supreme Court reversed both judgments.[69]

The government argued that because the arrest occurred in Mexico, the foreign country exception barred the claim.[70] The Court explained that the plaintiff's "arrest, however, was said to be "false," and thus tortious, only because, and only to the extent that, it took place and endured in Mexico. The actions in Mexico are thus most naturally understood as the kernel of a "claim arising in a foreign country,"[71] and barred from suit under the exception to the waiver of immunity."[72]

Conversely, the plaintiff and the circuit court argued that the suit should proceed under the "headquarters doctrine" since the arrest was planned and directed in the United States.[73] "Headquarters claims typically involve allegations of negligent guidance in an office within the United States of employees who cause damage while in a foreign country, or of activities which take place within a foreign country."[74] When the headquarters doctrine applies, the suit is not barred by the foreign country exception.[75]

The Supreme Court held that the foreign country exception bars all claims against the government based on any injury suffered in a foreign country, regardless of where the tortious act or omission that gave rise to the injury occurred.[76] According to the Court, the proximate cause "between domestic behavior and foreign harm or injury is not sufficient of itself to bar application of the foreign country exception to a claim resting on that same foreign consequence."[77] The Court expressed concern that the "headquarters

[65] Sosa v. Alvarez-Machain, 542 U.S. 692, 697-98 (2004).
[66] *Id.* at 698.
[67] *Id.* at 699.
[68] *Id.*
[69] *Id.*
[70] *Id.*
[71] *Id.* at 700-01.
[72] *Id.* at 701.
[73] *Id.*
[74] *Id.* (internal quotations omitted).
[75] *Id.*
[76] *Id.* at 700.
[77] *Id.* at 703-04.

doctrine threatens to swallow the foreign country exception whole, certainly at the pleadings stage."[78]

Just as the Court had done in *Spelar*, the Court rehearsed the legislative history of the foreign country exception and came to the same conclusion that the exception's main purpose was to shield the United States from liability according to the laws of other countries.[79] The Court did not provide an actual definition of "foreign country" for the purposes of the foreign country exception, relying more on its implied meaning.[80]

iii. *Meredith v. United States*

The facts of *Meredith v. United States* are quite similar to those in *Galvin v. United States*.[81] In *Meredith*, the plaintiff was seeking damages for an injury that occurred on embassy property in Bangkok, Thailand.[82] Like the Supreme Court in *Spelar* and *Sosa*, the 9th Circuit reviewed the legislative history of the foreign country exception, stating "[t]he words 'foreign country' are not words of art, carrying a fixed and precise meaning in every context."[83] Ironically, the 9th Circuit did not go further to define the "fixed and precise meaning" in the context of the foreign country exception, leaving still the ambiguity described in *Burnet*. Instead, the 9th Circuit went no further than to state that "[t]he phrase 'in a foreign country' is used in § 2680(k) with the meaning dictated by 'common sense' and 'common speech.'"[84] In the end, the 9th Circuit affirmed the district court's decision to dismiss the claim on summary judgment.[85]

E. Embassy Jurisdiction in the Criminal Context: Special Maritime and Territorial Jurisdiction - 18 U.S.C. § 7(3)

The lack of definitional specificity for "foreign country" and the courts' opinions regarding the foreign country exception become even more confusing when compared to the United States' Special Maritime and Territorial Jurisdiction found in 18 U.S.C § 7.

18 U.S.C. § 7(3) states that the "special maritime and territorial jurisdiction of the United States" includes "[a]ny lands reserved or acquired

---

[78] *Id.* at 703.

[79] *Id.* at 707.

[80] *See id.* at 700-01 ("Alvarez's arrest, however, was said to be 'false,' and thus tortious, only because, and only to the extent that, it took place and endured in Mexico. The actions in Mexico are thus most naturally understood as the kernel of a 'claim arising in a foreign country,' and barred from suit under the exception to the waiver of immunity.").

[81] *See* Meredith v. United States, 330 F.2d 9, 10 (9th Cir. 1964)*; see also* Galvin v. United States, 859 F.3d 71, 72 (D.C. Cir. 2017).

[82] *Meredith*, 330 F.2d at 10.

[83] *Id.*

[84] *Id.* at 11.

[85] *Id.*

for the use of the United States, and under the exclusive or concurrent jurisdiction thereof, or any place purchased or otherwise acquired by the United States by consent of the legislature of the State in which the same shall be, for the erection of a fort, magazine, arsenal, dockyard, or other needful building."[86] As discussed later, the Supreme Court has explicitly held that the clause "other needful building" *does* indeed include property procured for use by a United States' Embassy.[87]

F. Legislative History of the Special Maritime and Territorial Jurisdiction of the United States

The original version of 18 U.S.C § 7, passed in 1790, provided basic criminal laws for lands outside the jurisdiction of any sovereign nation, including the United States.[88] At the time the original version was enacted, the intent was "to prevent that detestable crime [murder] from finding harbor and impunity in places where no other law than that of the United States could reach to punish."[89] As the United States expanded its power and control, Congress continued to expand federal criminal jurisdiction.[90] By the nineteenth century, the special territorial jurisdiction of the United States included territory beyond the actual boundaries of the mainland United States.[91]

Congress understood criminal jurisdiction to extend to all lands claimed by the United States, without regard to a particular state, or even within the continental United States, when it granted jurisdiction through the single statute.[92] "Congress declined to assert jurisdiction over territories subject to the more comprehensive criminal codes of the states or self-governing territories," but "it showed no intent to limit jurisdiction on the basis of geography alone."[93] In 1940, Congress further expanded the Act's jurisdiction to include those lands under the concurrent authority of the United States.[94]

G. The Special Maritime and Territorial Jurisdiction in Case Law: United States v. Corey & United States v. Erdos

Although they are not the only cases addressing the special maritime and territorial jurisdiction of the United States, both *United States v. Corey*

---

[86] 18 U.S.C. § 7(3) (2018).
[87] *See* United States v. Erdos, 474 F.2d 157, 159 (4th Cir. 1973).
[88] United States v. Corey, 232 F.3d 1166, 1173 (9th Cir. 2000).
[89] *Id.* at 173-74.
[90] *Id.* at 1174.
[91] *Id.*
[92] *Id.*
[93] *Id.*
[94] *Id.*

and *United States v. Erdos* discuss crimes perpetrated on embassy property.[95] In both cases, the circuit court allowed the United States to exercise jurisdiction over the embassy.[96]

i. *United States v. Corey*

Corey, a United States citizen, lived abroad with his family while working for the U.S. Air Force as a civilian postmaster.[97] Corey ran the post office at the American Embassy in Manila, Philippines, and for several years prior, managed the office at the U.S. Air Force Base at Yokota, Japan.[98] In 1996, Corey's stepdaughter told her doctor that Corey had sexually abused her starting when she was fifteen.[99] After an investigation, the government charged Corey with aggravated sexual abuse and sexual abuse.[100] Corey was convicted on eight of eleven counts and sentenced to 262 months in prison.[101] On appeal, he challenged the district court's jurisdiction.[102]

The 9th Circuit in *Corey* conducts an in-depth analysis of what it means for a piece of property to be "reserved or acquired for the use of the United States."[103] "There is no requirement that the United States be an owner, or even an occupant, so long as the land has been set aside for the use of an instrumentality of the federal government."[104] Because the "State Department leased the apartment building from a private landlord for the purpose of housing our embassy personnel,"[105] "the lease runs without regard to the residence of a particular employee."[106] Because "the government pays rent and utilities, and provides security for the buildings,"[107] "it was an apartment acquired by the State Department for governmental use."[108]

Although the embassy remains the territory of the receiving state to a certain degree, diplomatic conventions disable the government from exerting effective control over the area.[109] The local police could not enter the premises to investigate crimes without the consent of the ambassador, nor could they prosecute Corey, or any other American member of the embassy staff.[110] The United States has the legal authority to regulate conduct on those

---

[95] *Id.* at 1183; United States v. Erdos, 474 F.2d 157, 160 (4th Cir. 1973).
[96] *Id.*
[97] *Corey*, 232 F.3d at 1169.
[98] *Id.*
[99] *Id.* at 1169.
[100] *Id.*
[101] *Id.*
[102] *Id.*
[103] *See id.* at 1177; *see generally* 18 U.S.C. § 7(3) (2018).
[104] *Corey*, 232 F.3d at 1177.
[105] *Id.*
[106] *Id.*
[107] *Id.*
[108] *Id.*
[109] *Id.* at 1183.
[110] *Id.*

grounds.[111] The Court concluded that the United States exercises concurrent, even primary, jurisdiction over the actions of United States nationals on both the Air Force base and the embassy property.[112]

ii. *United States v. Erdos*

In a case specifically dealing with United States' criminal law jurisdiction on embassy property, the Court of Appeals for the 4th Circuit explicitly held that the United States *can* exercise jurisdiction over embassy property.[113]

On American Embassy property in the New Republic of Equatorial Guinea, Alfred Erdos killed Donald Leahy.[114] Both were American citizens and embassy employees.[115] Erdos was tried and convicted of voluntary manslaughter in the District Court for the Eastern District of Virginia.[116] One of the issues on appeal was whether the district court had jurisdiction to try Erdos for a crime occurring on American Embassy property located in a foreign country.[117]

Ironically, the 4th Circuit applied almost identical reasoning to *allow* this jurisdictional reach to embassy property that the Supreme Court used to *deny* this kind of jurisdictional reach under the foreign country exception.[118] The 4th Circuit explicitly stated that "[t]he test, as to property within or without the United States, [is] one of practical usage and dominion exercised over the embassy or other federal establishment by the United States government."[119] The court further explained that the first and second clause of the statute[120] clearly intended to "create a jurisdictional category: lands reserved or acquired for the use of the United States under its exclusive or concurrent jurisdiction."[121]

The 4th Circuit held that 18 U.S.C. § 7(3) is a proper grant of "special" territorial jurisdiction embracing property acquired for the use of the United States' embassy and under its concurrent jurisdiction.[122] Clearly, courts can construe statutes in such a way as to extend the jurisdiction of the United States onto embassy properties. The question remains, however, as to

---

[111] *Id.*
[112] *Id.*
[113] United States v. Erdos, 474 F.2d 157, 160 (4th Cir. 1973).
[114] *Id.* at 158.
[115] *Id.*
[116] *Id.*
[117] *Id.*
[118] *See id.* at 160.
[119] *Id.* at 159.
[120] 18 U.S.C. § 7(3) (2018) ("Any lands reserved or acquired for the use of the United States, and under the exclusive or concurrent jurisdiction thereof…").
[121] *Erdos*, 474 F.2d at 160.
[122] *Id.*

why Congress and the courts have been so hesitant as to allow in a civil context what they have so freely given in a criminal context.

III. ANALYSIS

As the law stands right now, Kathy-Lee Galvin (or any foreign service member, for that matter) could be tried and convicted of murder in a United States Federal Court, under the jurisdiction of the United States, and according to the laws of the United States, as *Erdos* and *Corey* make clear.[123] Yet, Kathy-Lee Galvin was awarded *no relief* for severe injuries caused by the negligence of the United States government. She sued the United States in federal court, under the jurisdiction of the United States, and according to the laws of the United States.[124] In fact, if the family of Erdos' victim was to sue Erdos for wrongful death their claim, too, would be dismissed. Same set of operative facts, same location, dramatically different results.

A. Legal Problems of Applying the Foreign Country Exception on Embassy Property

It is quite possible that Congress has the same choice of law concerns that it had when it first enacted the FTCA. One particular reason courts have given for excluding embassies under the foreign country exception is that "obviously our embassy . . . has no tort law of its own"[125] and "[p]resumably the law applicable on these premises would be that of the receiving country."[126] An additional concern, according to Judge Sobeloff in *Meredith*, is "the absence of United States courts in such countries, with resulting problems of venue, and the difficulty of bringing defense witnesses from the scene of the alleged tort to places far removed."[127]

In the early days of the foreign country exception, courts were generally operating under the assumption that the negligence and the injury occurred in the same place[128], which is not quite true today. More recently, courts have focused on the site of the negligence, as opposed to that of the injury, to determine where the claim arose.[129] In Kathy-Lee Galvin's case, which would be true for other foreign service officers, it was the State Department *in* the United States that was negligent in selecting the housing.[130]

---

[123] United States v. Corey, 232 F.3d 1166 (9th Cir. 2000); *Erdos*, 474 F.2d at 157.
[124] *See* Galvin v. United States, 859 F.3d 71, 72 (D.C. Cir. 2017).
[125] Meredith v. United States, 330 F.2d 9, 10 (9th Cir. 1964).
[126] *Id.*
[127] *Id.* (quoting Burna v. United States, 240 F.2d 720, 722 (4th Cir. 1957)).
[128] *See, e.g.*, United States v. Spelar, 338 U.S. 217 (1949); *Meredith*, 330 F.2d at 9.
[129] McCracken, *supra* note 49, at 603.
[130] *See* Galvin v. United States, 859 F.3d 71 (D.C. Cir. 2017).

Furthermore, these same concerns arguably arise when a crime is committed on embassy property, and yet Congress has explicitly provided for United States law to reach those crimes.[131] For example, the murder in *Erdos* took place on American Embassy property in the New Republic of Equatorial Guinea; yet, Erdos was tried in the United States District for the Eastern District of Virginia and the appeal was heard in the United States Court of Appeals for the 4th Circuit.[132] Similarly, the crimes in *Corey* were perpetrated in the Philippines and Japan; yet, Corey was prosecuted and convicted in the United States District Court for the District of Hawaii, and his appeal was heard in the United States Court of Appeals for the 9th Circuit.[133] In the context of the FTCA, Congress can provide for how to handle civil claims arising on embassy property in much of the same way it dealt with how to handle criminal actions on embassy properties. Although there are certainly arguments to be made regarding a federal common law that encompasses embassies and United States' jurisdiction over such, the Supreme Court has held that "few areas, involving 'uniquely federal interests,' are so committed by the Constitution and laws of the United States to federal control that state law is pre-empted and replaced, where necessary, by federal law of a content prescribed. . . by the courts—so-called 'federal common law.'"[134] Clearly, jurisdiction over a United States embassy is an area of unique federal interests.

B. Practical Problems of Applying the Foreign Country Exception on Embassy Property

The practical problems of applying the foreign country exception on embassy property are even clearer than the legal problems, especially considering how many federal employees are affected by this bar. As of December 31, 2017, there were 13,678 foreign service employees, 9,441 FS and CS overseas employees, and 31 government agencies represented overseas.[135] In addition, the United States had 276 overseas posts, including 170 embassies.[136] In 2013, there were only *seven* countries in which the United States did not have any diplomatic presence: Antigua and Barbuda, Dominica, Grenada, St. Kitts and Nevis, St. Lucia, St. Vincent and the Grenadines, and Guinea-Bissau.[137] According to the current interpretation of the foreign country exception, each and every one of these people, if they

---

[131] *See* 18 U.S.C. § 7(3) (2018).

[132] United States v. Erdos, 474 F.2d 157, 158 (4th Cir. 1973).

[133] United States v. Corey, 232 F.3d 1166, 1169 (9th Cir. 2000).

[134] Boyle v. United Techs. Corp., 487 U.S. 500, 504 (1988) (citations omitted).

[135] U.S. Dep't of State, *Dep't of Human Resources Fact Sheet*, AM. FOREIGN SERV. ASS'N (Dec. 31, 2017), http://www.afsa.org/sites/default/files/1217_state_dept_hr_factsheet.pdf.

[136] *Id.*

[137] Amy Roberts, *By the Numbers: U.S. Diplomatic Presence*, CNN POLS. (May 9, 2013), https://www.cnn.com/2013/05/09/politics/btn-diplomatic-presence/index.html.

were injured overseas on embassy or consulate property, are barred from seeking recovery from the United States.

The legislative history makes it clear that Congress's purpose in enacting the FTCA was one of fair play and justice – in enacting the FTCA, Congress allowed claimants to recover against the United States in the same way as if they had been injured by private individuals.[138] How, then, can the FTCA be fulfilling its purpose by barring thousands of individuals employed on United States embassies from recovery? Factor in the number of civilians employed by the U.S. military, and that number grows exponentially.[139] As Kelly McCracken explained in her article, "sending Americans and their families abroad, as the United States government does with military and embassy personnel, then not allowing them to recover when injured by United States officials or employees is particularly unfair."[140]

C. Solutions to These Problems

Two solutions come to mind when thinking about how to solve the legal and practical problems that are created by barring all claims arising on embassy property.

The first solution: Congress should amend the FTCA's foreign country exception that essentially creates an exception-within-an-exception. This new exception should parallel the special maritime and territorial jurisdiction of the United States found in 18 U.S.C. § 7(3), which the courts have explicitly found extends to embassy property.[141]

The second, arguably more cumbersome solution: the Supreme Court can construe the foreign country exception to *exclude* embassy properties. This would, of course, first require a case to be filed in the district court, that gets appealed to the Court of Appeals, and then appealed to the Supreme Court. The Supreme Court would then need to grant certiorari – a rare and difficult feat. Nevertheless, it is not impossible.

i. Solution 1: Amend The Foreign Country Exception to Create An Exception Within An Exception That Parallels 18 U.S.C. § 7(3).

I am not denying that as the law currently stands, the United States is *not* liable for tort claims that arise on embassy property. I am arguing,

---

[138] McCracken, *supra* note 49, at 623.

[139] Indeed, as of June 2020 there are a reported 761,000 civilian employees of the Department of Defense and "224,000 combined personnel in over 170 countries." Kimberly Amadeo, *Department of Defense and Its Effect on the Economy*, BALANCE (Nov. 10, 2020), https://www.thebalance.com/department-of-defense-what-it-does-and-its-impact-3305982.

[140] McCracken, *supra* note 49, at 623.

[141] *See* United States v. Corey, 232 F.3d 1166 (9th Cir. 2000); United States v. Erdos, 474 F.2d 157, 158 (4th Cir. 1973).

however, that the United States *should* be liable for tort claims that arise on embassy property. I am also not denying the validity of the original enacting Congress' general policy reasons for not wanting the United States to be liable according to another country's laws. Nonetheless, the legislative history suggests that the *main* purpose for enacting the FTCA was for "fair play and justice."[142] How, then, can the statute really be living up to its main purpose of "fair play and justice" by excluding a sizeable population of the federal government's workforce?[143]

When Congress enacts legislation, there is generally a "presumption against extraterritoriality."[144] "The territorial presumption is . . . based on the common-sense inference that, where Congress does not indicate otherwise, legislation dealing with domestic matters is not meant to extend beyond the nation's borders."[145] However, in explaining the presumption against extraterritoriality, the 9th Circuit has stated that "the presumption does not apply where the legislation implicates concerns that are not inherently domestic."[146]

The foreign country exception clearly deals with "concerns that are not inherently domestic."[147] It is clear from the legislative history that in enacting the foreign country exception, Congress was driven primarily by protecting the United States from liability under the laws of another country.[148] There are, of course, choice of law questions that would have to be addressed if Congress were to expand the FTCA to allow claims arising on embassy property.[149] Nevertheless, there is nothing that expressly prohibits Congress from expanding the FTCA.[150] In fact, "no one challenges the power of Congress to extend the remedy provided by the Federal Tort Claims Act to persons injured on premises occupied by this nation's foreign embassies and consulates."[151] Congress *should* "extend the remedy provided by the Federal Tort Claims Act to persons injured on premises occupied by this nation's foreign embassies and consulates,"[152] and Congress has the legal authority to do so.[153]

Embassies are, in a way, "possessions" of the United States, making it clear that the applicable United States law should apply, at least when the injured party is a citizen of the United States.[154] The United States has a

---

[142] United States v. Spelar, 338 U.S. 217, 220-22 (1949).
[143] U.S. Dep't of State, *supra* note 135.
[144] *Corey*, 232 F.3d at 1170.
[145] *Id.*
[146] *Id.*
[147] *Id.*
[148] *See* United States v. Spelar, 338 U.S. 217, 221 (1949).
[149] *See id.*
[150] Meredith v. United States, 330 F.2d 9, 10 (9th Cir. 1964).
[151] *Id.*
[152] *See id.*
[153] *See id.*
[154] McCracken, *supra* note 49, at 630.

strong interest in permitting recovery by its own citizens, and narrowing the foreign country exception *not* to include embassy properties would better serve the interests of fair play and justice by permitting more meritorious claimants to recover under the FTCA.[155] Congress should include a section analogous to 18 U.S.C. § 7(3) that allows the FTCA to reach "[a]ny lands reserved or acquired for the use of the United States, and under the exclusive or concurrent jurisdiction thereof…"[156]

ii. Solution 2: The Supreme Court Can Construe The Foreign Country Exception To Not Reach Embassy Properties.

Even if Congress is not willing to narrow the exception to not include embassy property, the courts can read the statute in such a way as to not include embassy property. Like the foreign country exception, 18 U.S.C. § 7(3) does not explicitly mention anything about embassy properties.[157] Nevertheless, the 4th and 9th Circuits have read into the statute jurisdiction over crimes occurring on embassy property.[158] Just as the 4th Circuit did in *Erdos* and the 9th Circuit did in *Corey*[159], courts can construe the foreign country exception in such a way as to allow jurisdiction over claims arising on embassy property.

In *United States v. Corey*, the 9th Circuit explained that "embassy property remains the territory of the receiving state, and does not constitute [the] territory of the United States."[160] Nonetheless, "acknowledging the claims of the foreign government does not determine whether the United States exercises concurrent jurisdiction over that territory—particularly with regard to the actions of its own citizens."[161] The 9th Circuit further recognized that "[t]here is no question that domestic lands may fall under the concurrent jurisdiction of the state and federal governments."[162] "What matters is not whose law trumps in particular situations, but that there is a law-driven means for resolving any conflict."[163] Because the United States does in fact exercise concurrent jurisdiction over embassy properties, the Courts can construe the foreign country exception in such a way that it does not encompass embassy properties.

---

[155] *Id.* at 622.
[156] 18 U.S.C. § 7(3) (2018).
[157] *Id.*
[158] *See* United States v. Corey, 232 F.3d 1166, 1172 (9th Cir. 2000); United States v. Erdos, 474 F.2d 157, 158 (4th Cir. 1973).
[159] *Corey*, 232 F.3d at 1172.
[160] *Id.* at 1178 (quoting McKeel v. Islamic Republic of Iran, 722 F.2d 582, 588 (9th Cir. 1983).
[161] *Id.*
[162] *Id.* at 1180.
[163] *Id.*

IV. CONCLUSION

There is no reason that people like Kathy-Lee Galvin may be prosecuted according to United States law in United States Federal Courts for crimes committed on embassy property; yet have their claims dismissed when they attempt to recover for the government's negligence. Why is it that the same location would yield polar opposite results in two different legal contexts? Why is it that Kathy-Lee could be prosecuted according to United States law, under United States Jurisdiction, in a United States Federal Court if she *murdered* her husband in the Embassy housing, but she *cannot* recover damages according to United States law, under United States Jurisdiction, in a United States Federal Court after being crushed under housing supplied to her *by the United States*?

The legislative history makes it clear that when implementing the Federal Tort Claims Act, the Seventy-Ninth Congress was concerned about subjecting the United States to liability under the laws of other countries. It is well established that the foreign country exception was included in the Act specifically to combat this fear. As a result, the foreign country exception is so broadly written that it has come to encompass far more than the enacting Congress perhaps ever intended, and has led to some truly unfair outcomes—with the narrative described at the beginning of this comment being a prime example.

The law, as it currently stands, allows the United States to prosecute people for crimes committed on embassy property using the same explanation as it does for not allowing citizens to recover for torts committed on embassy property. If the Federal Tort Claims Act's main aim truly is "fair play and justice," then excluding such a sizeable portion of the federal workforce is certainly not fulfilling that purpose.

But it does not need to be this way. Despite the current state of the law regarding the FTCA's foreign country exception, the United States *can* exercise its jurisdiction on embassy property. Just as Congress has provided for jurisdiction over crimes committed on embassy property, it can also provide jurisdiction over torts committed on embassy property. Congress legally can, and should, provide for relief according to the FTCA for claims arising on embassy property. Since the United States exercises concurrent jurisdiction over embassy property, Congress can provide a route to relief according to the FTCA – no one doubts that fact.

There are many opportunities for further research surrounding the foreign country exception. The foreign country exception has already been examined in the context of the frontier of Antarctica,[164] as well as in the context of military bases.[165] But it can also be examined in an employment

[164] *See* Dean, *supra* note 28, at 553.
[165] *See, e.g.*, United States v. Spelar, 338 U.S. 217, 222 (1949).

context – foreign service officers injured overseas are barred from bringing claims against the United States as their employer. This issue will not likely come to rest until either Congress or the Supreme Court offers a clear definition of a foreign country, or specifically provides for what does, and does not, fall within the exception. Unfortunately, however, I do not think that is likely to happen anytime soon.