"THE RIGHT TO BE FORGOTTEN" AND ITS UNINTENDED CONSEQUENCES TO INTELLIGENCE GATHERING

Charlene C. Goldfield[*]

Social media has dramatically changed how we interact and communicate with one another. The reliance on social media has also sparked many international debates revolving around privacy. We have seen the enactment of the comprehensive privacy law in the European Union, the General Data Protection Regulation (GDPR), and the California Consumer Privacy Act (CCPA) in the United States—both enacted in 2018. In the GDPR, Article 17, known as the "Right to Be Forgotten" (RTBF) principle, allows for data subjects to request that their information be removed from online service providers like social media companies. In recent years, cases from the Court of Justice for the European Union have expanded these RTBF principles through three major cases: *Google LLC v. Commission nationale de l'informatique et des libertés (CNIL)*, *GC v. Commission nationale de l'informatique et des libertés (CNIL)*, and *Glawischnig-Piesczek v. Facebook*. This Article argues that the RTBF model will present unintended consequences to Open Source Intelligence (OSINT) by mandating online service providers to delete more data than necessary based on the pressures placed on these online service providers by the recent Court of Justice for the European Union (CJEU) cases. This will lead to problems in the Intelligence Community when obtaining open source intelligence especially when scrubbing social media information. This RTBF system will make it easier for terrorist groups, terrorist sympathizers or any other associated individuals to hide behind a process by which they can easily delete data that was not so easily removable before RTBF. Lastly, this Article proposes legal, procedural, and oversight solutions to address the issues caused by RTBF and OSINT.

---

* Charlene Collazo Goldfield is an attorney with the federal government and an LL.M. student in the National Security & Cybersecurity Law Program at George Washington University Law School. Charlene is also an Adjunct Faculty in the Public Administration Program at Florida International University. I would like to thank Professor Paul Rosenzweig for his advice and support. I would also like to thank my husband for his continued support of my educational and professional goals.

INTRODUCTION

The use of social networking has increased, dramatically, in the last few years. As of January 2019, Facebook Messenger documented about 1.3 billion users, meanwhile WhatsApp documented 1.5 billion users.[1] With the increased use of social media, more publicly available information on the internet has assisted with anticipating when future terrorist attacks might occur and the crucial location sites where they might take place in order to prevent them.[2] This has made Open Source Intelligence (OSINT)—information publicly-available for intelligence purposes—more critical than ever. Eighty percent of information obtained for intelligence mission purposes is "publicly available."[3]

One crucial example is a U.S. military airstrike conducted in 2014 over an Islamic State bomb factory. The U.S. military was able to obtain the precise location of this factory from a "selfie" photograph of the building posted on one of the jihadi members' social media.[4] There are several other instances when OSINT has greatly assisted with counterintelligence operations. With such a dependable reliance on OSINT, it is important that OSINT is not only supported, but encouraged within the Intelligence Community (IC).

The relationship between national security and privacy has always been marked with tension, especially in the area of intelligence gathering. This sentiment can be attributed to the rapid transformation of digital incorporation into society.[5] But the Edward Snowden leaks pushed more

1. Maya E. Dollarhide, *Social Media Definition*, INVESTOPEDIA (Sept. 6, 2020), https://www.investopedia.com/terms/s/social-media.asp [https://perma.cc/GZ9G-JDR8].

2. Sofia Charania, *Social Media's Potential in Intelligence Collection*, 33 AM. INTELL. J. 94, 96 (2016).

3. *Id.* at 94.

4. Cameron Colquhoun, *A Brief History of Open Source Intelligence*, BELLINGCAT (July 14, 2016), https://www.bellingcat.com/resources/articles/2016/07/14/a-brief-history-of-open-source-intelligence/ [https://perma.cc/S58Q-L529].

5. Julie E. Cohen, *Surveillance versus Privacy*, *in* CAMBRIDGE HANDBOOK OF SURVEILLANCE LAW 455 (David Gray & Stephen E. Henderson eds., 2017).

people to feel uncertain about the intelligence community.[6] This uncertainty was mostly felt in the European Union (EU). Before the Snowden leaks, discussions on the enactment of a comprehensive privacy law that would replace Directive 95/46/EC on the Protection of Individuals with Regard to the Processing of Personal Data and on the Free Movement of Such Data (the "Directive")[7] had faded.[8]

However, in the wake of the Snowden leaks in June of 2013,[9] the European Parliament and Council of the EU enacted the General Data Protection Regulation (GDPR) in 2016 with the specific design to repeal the previous directive.[10] The Right to Be Forgotten (RTBF), codified in the GDPR under Article 17, is rooted in the preservation of privacy protections by allowing individuals to request a process by which their data can be deleted from companies that process or control data.[11]

The RTBF principle first arose from the Court of Justice for the European Union (CJEU) decision in *Google Spain SL. v. Agencia Española de Protección de Datos*[12] (hereinafter referred to as *Google v. Spain*). This case mandated that commercial search companies like Google remove links that led to information on private individuals following a search made about a private individual's name.[13] Ultimately, this decision would require search engine platforms to establish RTBF procedures that would allow individuals to remove data about themselves.

The CJEU has continued to expand the RTBF theory with three recent decisions: *Google LLC v. Commission nationale de l'informatique et des*

---

6. Rachel L. Brand, *Balance in Intelligence Gathering and Privacy*, THE HILL (Dec. 15, 2015), https://thehill.com/blogs/congress-blog/homeland-security/263143-balance-intelligence-gathering-and-privacy.

7. Council Directive 95/46, 1995 O.J. (L 281) 1 (EC), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A31995L0046 [https://perma.cc/3NL3-8ZK8].

8. *See* Agustín Rossi, *How the Snowden Revelations Saved the EU General Data Protection Regulation*, 53 THE INT'L SPECTATOR, no. 4, 2018, at 95, 104 (discussing the political landscape before the Snowden revelations regarding privatelegislation).

9. Paul Szoldra, *This is everything Edward Snowden revealed in one year of unprecedented top-secret leaks*, BUS. INSIDER (Sept. 16, 2016, 8:00 AM), https://www.businessinsider.com/snowden-leaks-timeline-2016-9 [https://perma.cc/37ME-6N9G] (stating, "In June 2013, The Guardian reported the first leak based on top-secret documents that then 29-year-old Edward Snowden stole from the National Security Agency.").

10. Regulation 2016/679, art. 94, 2016 O.J. (L 119) 1 (EU), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A02016R0679-20160504 [https://perma.cc/GF7S-RC22] [hereinafter GDPR].

11. *Id.* art. 17.

12. Case C-131/12, Google Spain SL v. Agencia Española de Protección de Datos, ECLI:EU:C:2014:317 (May 13, 2014) https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62012CJ0131 [https://perma.cc/X5MT-JK25] [hereinafter Google v. Spain].

13. *Id.* ¶ 100(3).

libertés (CNIL),[14] *GC v. Commission nationale de l'informatique et des libertés (CNIL)*[15] (as these are two separate decisions involving Google and CNIL, these two decisions will hereinafter be referred to as *Google I* and *Google II* respectively), and *Glawischnig-Piesczek v. Facebook Ireland Ltd.* (hereinafter referred to as the *Facebook* case).[16] In *Google I*, the CJEU determined that injunctions requiring internet service platforms to take down personal information of European citizens did not apply globally.[17] While this decision seemed like a win for internet platform companies, in reality, the CJEU left open the possibility for EU member states to legislate a global takedown requirement.[18] As for *Google II*, the Court created a notice-and-delist regime for sensitive data and determined certain actions to take on content display by search engines.[19] In the *Facebook* case, the Court determined that social media sites are subject to RTBF regulations and that delisting obligations can be mandated globally.[20]

A point that can be obtained from the RTBF cases is that personal data is an extension of the individual—a blurred line between the kinetic and digital world. While it is understandable that the EU and its courts would strongly support RTBF, there is an unintended consequence that RTBF will cause if it is not properly addressed—a predicament that occurs when courts are utilized to create policy. The RTBF system will pose problems for OSINT by mandating data providers to delete more data than necessary according to the pressures placed on them by the recent CJEU cases. This will lead to problems in the Intelligence Community when conducting OSINT efforts, especially when scrubbing social media information. This RTBF system will make it easier for terrorist groups, terrorist sympathizers or any other associated individuals to hide behind a process by which they can easily delete data that was not so easily removable before RTBF.[21]

---

14. Case C-507/17, Google LLC, successor in law to Google Inc. v. Commission nationale de l'informatique et des libertés, ECLI:EU:C:2019:772 (Sept. 24, 2019) [hereinafter Google I].

15. Case C-136/17, GC v. Commission nationale de l'informatique et des libertés, ECLI:EU:C:2019:14 (Jan. 10, 2019), https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX:62017CC0136 [https://perma.cc/E4WS-NYG2] [hereinafter Google II].

16. Case C-18/18, Glawischnig-Piesczek v. Facebook Ireland Ltd., ECLI:EU:C:2019:821 (Oct. 3, 2019), https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A62017CJ0507 [https://perma.cc/XNH4-GZ6C] [hereinafter Facebook].

17. Google I, *supra* note 14, ¶ 64.

18. *Id.* ¶ 72.

19. Google II, *supra* note 15, ¶¶ 62–66.

20. Facebook, *supra* note 16, ¶¶ 37, 41, 50.

21. *See* Lexie N. Johnson, *Ctrl + Shift + Delete: The GDPR's Influence on National Security Posture*, COUNCIL ON FOREIGN RELS.: NET POL. (Oct. 8, 2019), https://www.cfr.org/blog/gdpr-influence-national-security-posture [https://perma.cc/T6HE-M925] (arguing that data collection efforts will be complicated by the "right to be forgotten" principle under GDPR).

This Article proposes three legal, procedural, and oversight solutions to mend the issues caused by RTBF and OSINT. An oversight model would assist with the processing side of RTBF claims made by individuals. By creating a data monitoring committee, similar to the Global Internet Forum to Counter Terrorism (GIFCT),[22] the ultimate decision to de-list or delete content would not rest solely in the hands of a data processor or Data Protection Authority (DPA). To address international differences in privacy standards and intelligence gathering, EU member states and the U.S. could follow a cooperation model solely concentrated on intelligence gathering, similar to the CLOUD Act model entered into between the United States (U.S.) and the United Kingdom (U.K.).[23] If no agreement is entered into with specific EU member states, then no intelligence gathering information can be obtained or received on that specific member states' person. Lastly, RTBF would not be applicable to an EU member state if there is a national security exemption as dictated by Article 23 of the GDPR.[24] As it stands, the national security exemption is not well defined, and it is unclear when it can be exercised. With only two years of GDPR enforcement, there has not been much precedent on how and when these exceptions can come into effect. These proposed solutions could assist in resolving the unintended consequence between OSINT and RTBF.

I. DISCUSSIONS ON GDPR, RTBF AND OSINT

A. *The GDPR Process and its Extraterritorial Reach*

The right to privacy first began to make headway into international law, through the enactment of Article 12 of the Universal Declaration of Human Rights in 1948, which briefly noted that an individual should not be "subjected to arbitrary interference with his privacy."[25] Then, in 1950, the European Convention of Human Rights enacted Article 8, which noted "[e]veryone has the right to respect for his private and family life . . ." and continued, "[t]here shall be no interference by a public authority with the exercise of this right . . . ."[26] Lastly, in 1966, Article 17 of the International Covenant on Civil and Political Rights provided that "[n]o one shall be subjected to arbitrary or unlawful interference with his

22. *Membership*, GLOB. INTERNET F. TO COUNTER TERRORISM, https://gifct.org/membership/ [https://perma.cc/6F4E-8PSX].

23. *U.S. And UK Sign Landmark Cross-Border Data Access Agreement to Combat Criminals and Terrorists Online*, U.S. DEP'T OF JUST. (Oct. 3, 2019), https://www.justice.gov/opa/pr/us-and-uk-sign-landmark-cross-border-data-access-agreement-combat-criminals-and-terrorists [https://perma.cc/R2LJ-XXFG] [hereinafter U.S. and U.K. Agreement].

24. GDPR, *supra* note 10, art. 23.

25. G.A. Res. 217 (III) A, Universal Declaration of Human Rights, art. 12 (Dec. 10, 1948).

26. Convention for the Protection of Human Rights and Fundamental Freedoms art. 8, Sept. 3, 1953, 213 U.N.T.S. 222.

privacy . . . ."[27] These provisions have been considered to be "broad and vague,"[28] however, it was not until 2013 that the United Nations passed a resolution specifically addressing the right to privacy in the digital age.[29]

As a result of Edward Snowden's shocking release of highly classified information obtained by the U.S. National Security Agency (NSA), the U.N. was pressed to address this issue.[30] The treatment of privacy between the EU and U.S. is vastly different. The EU categorizes privacy into data protection and private life.[31] The EU approach to regulating privacy is "comprehensive" and "overarching";[32] this is why the GDPR has been seen as the next best thing for data protection in the EU—it applies broadly and brings together all EU member states. In contrast, the U.S. defines privacy broadly and is regulated more sectoral.[33] These differences are important to consider because data is borderless and fluid, and cooperation among nation states is extremely important.

Within the EU context, before the GDPR, the Directive was adopted and allowed for EU member states to enact their own data protection legislation, while serving as an overarching guide.[34] The Directive created gaps in the law and introduced problems with enforcement among the EU member states.[35] The GDPR was enacted to address all these issues and strengthen data protection among the EU member states.[36] While the GDPR is expansive, it allows member states to enact their own derogations or supplemental legislation that pertain to certain national needs, which includes national security.[37] These derogations are acceptable, so long as it "respects the essence of fundamental rights and freedoms and is a necessary and proportionate measure in a democratic

27. G.A. Res. 2200 (XXI) A, International Covenant on Civil and Political Rights, art. 17 (Dec. 16, 1966).

28. Marko Milanovic, *Human Rights Treaties and Foreign Surveillance: Privacy in the Digital Age*, 56 HARV. INT'L L. J. 81, 83 (2015).

29. G.A. Res. 68/167, The Right to Privacy in the Digital Age, at 2 (Dec. 18, 2013).

30. *United Nations Recognition of Privacy*, PRIV. INT'L (May 2, 2018), https://privacyinternational.org/impact/united-nations-recognition-privacy [https://perma.cc/2YPD-AY22].

31. H. Jacqueline Brehmer, *Data Localization: The Unintended Consequences of Privacy Litigation*, 67 AM. UNIV. L. REV. 927, 934 (2018).

32. *Id.*

33. *Id.*

34. Chris Jay Hoofnagle et al., *The European Union General Data Protection Regulation: What Is and What It Means*, 28 INFO. & COMMC'N. TECH. L. 65, 70–71 (2019).

35. *Id.* at 71.

36. *Id.*

37. Ali Cooper-Ponte, *GDPR Derogations, ePrivacy, and the Evolving European Privacy Landscape*, LAWFARE (May 25, 2018, 7:00 AM), https://www.lawfareblog.com/gdpr-derogations-eprivacy-and-evolving-european-privacy-landscape [https://perma.cc/PT6T-3GSH].

society."[38] Even the RTBF provision of the GDPR has its own derogation applicability within Article 17.[39]

GDPR applies broadly to personal data—defined as any "information relating to an identified or identifiable natural person."[40] An identifiable natural person, known as the data subject, is "one who can be identified, directly or indirectly."[41] This means that it is not just personal identifiable information (PII) that must be protected.[42] Sensitive data, such as racial or ethnic origin, political opinion, biometrics or medical information etc., are all denoted under the "special categories" of data described in Article 9 of the GDPR.[43] Once personal data is processed, then GDPR requirements will be applicable.[44] Processing of data is performed by a data controller or processor and is broadly defined as follows:

> any operation or set of operations which is performed on personal or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.[45]

Data is only allowed to be processed if it meets at least one of six justifications under Article 6, which include consent by the data subject; legal obligation requires it; or there exists a legitimate interest.[46] One thing to note is that the "legitimate interest" justification does not necessarily apply as a blanket approval for online service providers.[47] The recent RTBF cases did not allow for a blanket approval to utilize this catch-all provision for avoiding the limitations to processing data.[48] Sensitive data is defined separately from personal data and several strict exceptions apply to its processing, including explicit consent of the data subject or the information has been manifestly made public by the data

38. GDPR, *supra* note 10, art. 23(1).
39. *Id.* art. 17(3)(a).
40. *Id.* art. 4(1).
41. *Id.*; Hoofnagle et al., *supra* note 34, at 72.
42. Hoofnagle et al., *supra* note 34, at 72.
43. GDPR, *supra* note 10, at art. 9(1).
44. Hoofnagle et al., *supra* note 34, at 72.
45. GDPR, *supra* note 10, at art. 4(2).
46. *Id.* art. 6(1)(a), (c), and (f).
47. Hoofnagle et al., *supra* note 34, at 81 (noting that a legitimate interest must be "explicitly disclosed").
48. *See* Daphne Keller, *The Right Tools: Europe's Intermediary Liability Laws and the EU 2016 General Data Protection Regulation*, 33 BERKELEY TECH. L. J. 297, 322 (2018) (explaining how this "concept is a slim reed upon which to rest the entire edifice of OSP operations.").

subject themselves.[49] Regardless, the GDPR is applicable whether the data is public or private.[50]

The GDPR assigns distinctions between individuals involved in the processing of personal and sensitive data, which affords them with varying legal obligations. Data controllers are the "entities that hold personal data and decide what to do with it," while data processors hold the personal data, waiting for instructions from the controller on what to do with the data.[51] Controllers have more responsibility, and so they have more legal obligations than processors.[52] The role of controller and processor provides a more fluid relationship between traditional companies that incorporate data as part of their business model, however, for platforms like Twitter, Facebook and Google, it dictates a more complex relationship.[53] Not only do these providers generate back-end user generated data like profiles, logs and user behavior, they also process content created and shared by users.[54] This dual relationship can prove to be difficult to regulate under a traditional data protection model like RTBF. Applying such a broad categorization to popular online platforms prove that the GDPR and RTBF principles were not meant to be applied broadly without understanding the consequences it could present. The most significant aspect of the GDPR is the hefty fine of up to £20,000,000 plus other administrative fines if data controllers or processors do not abide by these regulations.[55]

The GDPR applies extraterritorially under Article 3, which considers the establishment or the targeting involved.[56] There are three requirements under the establishment criteria, which are: (1) there must be some establishment of a controller or processor existing in the EU; (2) there must be the "existence of processing in the context of the activities of such establishment"; and (3) the understanding that neither the location

49. GDPR, *supra* note 10, at art. 9(2)(a) and (e). Sensitive data consists of racial or ethnic data; political opinions; religious or philosophical beliefs; or trade union memberships or biometric data. *Id.* art. 9(1).

50. Hoofnagle et al., *supra* note 34, at 73.

51. Keller, *supra* note 48, at 307.

52. *Id.* The distinction between controller and processor is important because compliance rests on the controller and the application of national law for purposes of data processing will be determined by where the controller is located. Article 29 Data Protection Working Party, *Opinion 1/2010 on the Concepts of "Controller" and "Processor"*, 00264/10/EN WP 169, at 5 (adopted Feb. 16, 2010), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2010/wp169_en.pdf [https://perma.cc/FHE6-URBB].

53. *See generally* Keller, *supra* note 48, at 308.

54. *Id.* at 308.

55. GDPR, *supra* note 10, art. 83.

56. *Id.* at art. 3; Lydia F. de la Torre, *Territorial Scope of EU Data Protection Law*, MEDIUM (Nov. 24, 2018), https://medium.com/golden-data/territorial-scope-of-eu-data-protection-law-d46c13eba23b [https://perma.cc/2T77-3HJT].

of the processing nor the location of the data subject are relevant.[57] If no establishment exists, GDPR still applies via the targeting criterion which only requires that the data subject be located in the EU and that the activities conducted by either controllers or processors offer goods and services or utilize monitoring as their services.[58]

In summary, it does not matter whether the company or its data is not located in the EU. Additionally, "the absence of an establishment in the Union does not necessarily mean that a data controller or processor established in a third country would be excluded from the territorial scope of EU data protection law."[59] It does not matter whether the data is located in the U.S. or the data controller or processor is located in the U.S.; GDPR could still be applicable.

B. *The RTBF Process and its Derogation Under National Security*

Article 17 spells out the RTBF procedure, which allows for data subjects "to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay" as long as one of several factors apply.[60] The RTBF procedure is not listed together under one section of the GDPR. Instead, they are "cobbled together from various provisions—many of which are ambiguous."[61] A request would most likely be handled as follows:

1. The online service provider receives the RTBF request.
2. If requested by the data subject, the data can be temporarily suspended or "restricted" from public access.
3. The claim is reviewed for its validity. If it is valid, then the content is de-listed or erased. If invalid, the content is placed back into public view.
4. The online service provider informs the requester of the outcome and communicates the removal request to other controllers processing the same data.
5. If requested, the online service provider provides the

57. *Id.*

58. *Id.*

59. European Data Protection Board, Guidelines 3/2018 On The Territorial Scope of the GDPR 13 (2020), https://edpb.europa.eu/sites/edpb/files/files/file1/edpb_guidelines_3_2018_territorial_scope_after_public_consultation_en_1.pdf [https://perma.cc/DZ8G-EN6B] [hereinafter EDPB Guidelines].

60. GDPR, *supra* note 10, at art. 17(1).

61. Keller, *supra* note 48, at 327.

contact details or identification information about the user who posted the removed content.

6. In most circumstances, the online service provider will not be allowed to tell the accused user that the content has been delisted or erased and the user has no opportunity to object.

7. Online service providers could disclose information about removals, but not individual instances. [62]

Although the wording is focused on public information, it does not necessarily mean that it would not apply to back-end and private data.[63] Focusing on the language in Article 21(1) of the GDPR, it implies that decisions whether to keep content are to be based on "compelling legitimate grounds."[64] In other words, "[i]t requires controllers to erase only to the extent that there are 'no overriding legitimate grounds' to continue processing," denoting a very low standard of review.[65]

The RTBF statute denotes that requests must be addressed "without undue delay,"[66] which may impose pressure on controllers and processors. However, one thing to note is the ability for member states to derogate from these obligations as directed under Article 17(3)(a).[67] Derogations allow member states to exercise their ability to enact amended legislation on an aspect of an agreement.

Currently, only France and Germany have derogated from Article 17.[68] Austria, Czech Republic, The Netherlands, and the United Kingdom have not exercised any derogation rights on the matter.[69] France's amended version of RTBF dictates that data controllers must respond or delete requests within one month of the filed request, and Germany exempts controllers from the obligation to erase personal data "managed through non-automatic data processing if it is deemed impossible or it is

62. *Id.* at 327–28.

63. *Id.* at 327 ("The steps are generally sensible for back-end data removals, such as requests to delete accounts, logs, or profiles.").

64. *See* GDPR, *supra* note 10, art. 17(1) ("The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the data subject for the establishment, exercise or deference of legal claims.").

65. *Id.* at 334.

66. GDPR, *supra* note 10, art. 17(1).

67. GDPR, *supra* note 10, art. 17(3)(a) ("3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary: (a) for exercising the right of freedom of expression and information;").

68. *A State-by-State Guide to GDPR Member State Derogations*, FOCAL POINT DATA RISK, https://go.focal-point.com/guide-to-gdpr-member-state-derogations [https://perma.cc/N6SL-MCM8] (last visited Nov. 10, 2020).

69. *Id.*

considered to be of high effort with low interest from data subject to erase."[70]

There is not much explanation as to the statutory construction of Article 17. In fact, the Article 29 Working Party—set up as an advisory group for the GDPR[71]—did not have much discussion on the RTBF topic other than its guidelines based on the *Google v. Spain* decision.[72] The group noted "the ruling [was] specifically addressed to generalist search engines, but that does not mean that it [could not] be applied to other intermediaries."[73] However, the Working Party does not provide much guidance on what is a "necessary and proportionate measure" for which a legislature can deviate from the GDPR, as proscribed in Article 23, in the name of "national security."[74]

Member states can derogate from these regulations under a national security need, so long as it "respects the essence of the fundamental rights and freedoms" as prescribed under Article 23.[75] In fact, Recital 16 to the GDPR reiterates how the GDPR does not apply to activities outside of EU law, such as those concerning national security activities.[76] But, Recital 16 is not the only reason why the GDPR does not apply to national security matters; the Treaty on European Union dictates under Article

---

70. *Id.*

71. The Article 29 Working Party was replaced with the European Data Protection Board as of May 25, 2018. European Comm'n, *The Article 29 Working Party Ceased to Exist As of 25 May 2018* (Nov. 6, 2018), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=629492 [https://perma.cc/8JMR-ZHY6].

72. Article 29 Working Party, *Guidelines on the Implementation of the Court of Justice of the European Union Judgment on "Google Spain and Inc. v. Agencia Espanola de Protección de Datos (AEPD) and Mario Costeja González" C-131/12*, 14/EN WP 225, at 5 (adopted Nov. 26, 2014), https://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=667236 [https://perma.cc/4SLQ-LJZV] [hereinafter WP *Guidelines*].

73. *Id.* at 8.

74. GDPR, *supra* note 10, art. 23(1)(a); *see also* Article 29 Working Party, *Working Document on Surveillance of Electronic Communications for Intelligence and National Security Purposes*, 14/EN WP 228, at 40, 45, 50 (adopted Dec. 5, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp228_en.pdf [https://perma.cc/4RL9-FCX6] [hereinafter WP *Surveillance*] (noting how the discussions on "necessary and proportionate" focus on the U.S. intelligence law landscape and how "the rule of law and the courts require restrictions to fundamental rights to be limited to what is strictly necessary and proportionate, specific and codified in law.").

75. GDPR, *supra* note 10, art. 23(1)(a).

76. *Recital 16: Not applicable to Activities Regarding National and Common Security*, GDPR.EU, https://gdpr.eu/recital-16-not-applicable-to-activities-regarding-national-and-common-security/ [https://perma.cc/JWB7-F45H] (last visited Feb. 17, 2021) [hereinafter *Recital 16*]; "Recitals found in the document provide context and greater depth of meaning to the Articles. Thus, both the Recitals and Articles are inexorably bound and must be taken together in order to understand the scope, reach, and intention of the GDPR." *What Are GDPR Recitals?*, RSI SECURITY (June 20, 2018), https://blog.rsisecurity.com/what-are-gdpr-recitals/ [https://perma.cc/M78U-PS97].

4(2) that national security is the sole responsibility of each member state and EU law cannot legislate on the matter.[77]

However, the Working Party does agree with the consensus that no true definition of national security exists.[78] Treaties seem to differentiate between terrorism and national security, and case law has been broad on the issue.[79] Instead, the Working Party has suggested that determining whether something falls under this exemption cannot be stripped down to a legal argument.[80] Instead, it should "take account of the political situation at the time the 'choice' is made, as well as the relevant actors."[81] These national security interpretations are reserved only for EU member states. When it involves a third party, like the U.S., it becomes even more unclear.

The national security exemption can be explained into three scenarios: applying only to EU member states; applying to the EU and U.S. as a joint security issue or applying to a security issue occurring in the U.S., but it involves an individual residing in the EU. The first scenario is self-explanatory as each EU member state would apply its own national security law. As to the second scenario, the national security exemption may not extended to both countries' actions, but the EU member state would have to demonstrate "why and how the national security interests coincide and thus exclude the application of EU law."[82] When companies work closely with government agencies on intelligence matters, the Working Party has advised the following:

> [C]ompanies need to be aware that they may be acting in breach of European law if intelligence services of third countries gain access to the data of European citizens stored on their servers or comply with an order to hand over personal data on a large scale. In that regard, companies may find themselves in a difficult position in deciding whether they comply with the order to supply personal data on a large scale or not: in either case they are likely to be in breach of European or third country law. Enforcement action against these companies in particular should not be excluded in situations where data controllers have willingly and

77. Consolidated Version of the Treaty on European Union art. 4(2), Oct. 26, 2012, 2012 O.J. (C 326) 18, https://eur-lex.europa.eu/resource.html?uri=cellar:2bf140bf-a3f8-4ab2-b506-fd71826e6da6.0023.02/DOC_1&format=PDF [https://perma.cc/UH5P-34LF].

78. WP *Surveillance*, *supra* note 74, at 22.

79. *Id.* at 22–24.

80. *Id.* at 24.

81. *Id.*

82. Article 29 Working Party, *Opinion 04/2014 on Surveillance of Electronic Communications for Intelligence and National Security Purposes*, 819/14/EN WP 215, at 7 (adopted Apr. 10, 2014), https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2014/wp215_en.pdf [https://perma.cc/2ASX-QPYQ].

> knowingly cooperated with intelligence services to give them access to their data.[83]

Since EU case law has not been too clear on what could constitute national security,[84] the third scenario could be guided by the extraterritorial trigger of the GDPR and the scant amount of case law.

As has been shown, many questions remain unanswered, such as, would a showing of an interconnected relationship still apply if another third country along with the U.S. is involved? Does the joint involvement involve issues where a third or fourth country might be involved? Obtaining a comprehensive definition of national security could address these questions and would help determine if EU member states can derogate from RTBF provisions as a national security need.

1. The Legal Landscape of RTBF

In the *Google v. Spain* case, the CJEU did not provide much instruction when it required Google to honor RTBF requests by "remov[ing] data that is inaccurate or 'inadequate, irrelevant or no longer relevant, or excessive in relation to the purpose of the processing, even if the information is true or causes no prejudice to the data subject.'"[85] This was an unclear amount of power provided to search engine platforms.

The *Google I* case focused on the removal of search result links that were related to an individual's name search.[86] Google removed the links from the individual's member country interface—France.[87] Google then instituted a geo-blocking of the individual's information based on the region.[88] The French Commission nationale de l'informatique et des libertés (CNIL) did not believe Google's actions were enough and so,

---

83. *Id.*

84. Rotaru v. Romania, App. No. 28341/95, ¶ 57 (May 4, 2000), http://hudoc.echr.coe.int/eng?i=001-58586 [https://perma.cc/U3DZ-46NK] (holding that data collected has to be relevant to national security purpose, and that the law should define "the kind of information that may be recorded, the categories of people against whom surveillance measures . . . [and] limits on the age of information held or length of time for which it may be kept."); *see* WP *Surveillance*, *supra* note 73, at 26 ("The claim that the national security interest of a third country aligns with an EU Member States' own national security interest should only be accepted if it is properly justified to the relevant authorities on a case-by-case basis."); *see also* Theresa Papademetriou, *Foreign Intelligence Gathering Laws: European Union*, THE LIBR. OF CONGRESS (Dec. 2014), https://www.loc.gov/law/help/foreign-intelligence-gathering/european-union.php#_ftnref43 [https://perma.cc/9C3U-CPWS] (explaining that the CJEU has no standing to review legal challenges to intelligence operations but the European Court of Human Rights (ECHR) can conduct such a review as the ECHR's view is one of a low standard by which the "mere existence of legislation allowing secret surveillance constitutes an interference with private life . . . .").

85. Keller, *supra* note 48, at 314; *see also*, Google v. Spain, *supra* note 12, ¶¶ 92–94.

86. Google I, *supra* note 14, ¶ 30.

87. *Id.* ¶ 31.

88. *Id.* ¶¶ 31–32.

they required them to apply a global de-listing.[89] The CJEU determined that Google was subject to GDPR regulations as an "operator who has one or more establishments in the territory of the Union in the context of activities involving the processing of personal data . . . regardless of whether that processing takes place in the Union or not."[90] The CJEU also created the general rule that the rights of individuals to the RTBF process would override economic interest of operator and general public access unless the individual interfaced with the public.[91] This would indicate that there is a low bar for data subjects and a high bar for internet search engines when it comes to RTBF procedures.

While Google and freedom of speech advocates rejoiced to the fact that the CJEU did not apply RTBF requirements extraterritorially, it still left the door wide open for EU member states to legislate on the issue by advocating that "EU law does not currently require that the de-referencing granted concern all versions of the search engine in question, it also does not prohibit such a practice."[92] Even if the EU member states considered legislation on this issue, they would still need to remember that RTBF requires a balancing test—the privacy of the individual versus the interests of the public.[93] Regardless, this one takeaway would allow for EU member states to exercise their opportunity to enact a global injunction of information that could incidentally affect intelligence gathering.

In the *Google II* case, it should be noted that the search result listings that were required to be removed were not illegal nor did the listings contain defamatory content.[94] Instead, the listings were links to the following: a YouTube video of a satirical photo montage;[95] a newspaper article that quoted an individual in his former capacity as a Scientology employee;[96] a newspaper article of an individual's judicial investigation into political funding mishaps;[97] and a newspaper article referencing an individual's criminal sentencing hearing.[98] Most of the factual information in the claims brought against the CNIL and Google dealt with what the GDPR defines as sensitive data under Article 19, which involves

89. *Id.* ¶ 32.

90. Google I, *supra* note 14, ¶ 48. This was important because in the previous ruling of *Google v. Spain* the GDPR had not been in effect.

91. *Id.* ¶ 45.

92. *Id.* ¶ 72.

93. See GDPR, *supra* note 10, art. 17.

94. Google II, *supra* note 15.

95. *Id.* ¶ 26.

96. *Id.* ¶ 27.

97. *Id.* ¶ 28.

98. *Id.* ¶ 29.

political opinions, religious beliefs and other general identifying information.[99]

The important takeaway from this case was the notice and takedown procedure that was created for sensitive data, which in the realm of OSINT, can be considered pieces of information that can create a mosaic of crucial information within the intelligence gathering realm.[100] Furthermore the *Google II* case is the expansive interpretation of the balancing test—privacy rights versus public interests, especially as applied to sensitive data.[101] If the public's interest in the information outweighs the privacy interest, then it needs to evaluate whether keeping the link is *strictly necessary* for preserving the public interest.[102] If the information is strictly necessary, then the search engine will need to adjust the list of results in a way that shows an overall picture—for instance, if the search results only mention an arrest or conviction, but no charges were ever filed, the criminal conviction was overturned, or the individual was not found guilty, that information would need to be added to the list of results.[103] An example of this in the case would be the claim brought by B.H. regarding search results displaying articles that he was questioned in a judicial investigation opened in June 1995, but not displaying articles mentioning the outcome of the investigation in which he was discharged and the proceedings were closed.[104]

However, what the definition or standards of strictly necessary might be are not quite clear. Oddly enough, the de-listed information discussed in this case was mostly public information that a public audience would want to know (i.e., political campaign violations or criminal trials), although this could be up for interpretation. Yet, the CJEU believed a RTBF decision should be based on a case-by-case interpretation where the bar is set too high for the public's interest.[105]

The *Facebook* case is the most controversial as it dealt with the removal of Facebook posts and comments made against a former public official, Eva Glawischnig-Piesczek.[106] The Austrian lower court felt the posts were harmful to Glawischnig-Piesczek's reputation.[107] Based on the lower court's ruling, Glawischnig-Piesczek asked Facebook to delete the posts, but Facebook refused as she was not the individual who published the comments.[108] The questions posed to the CJEU were threefold: First,

99. See GDPR, *supra* note 10, art. 19.
100. Google II, *supra* note 15, ¶¶ 62–66.
101. *Id.* ¶ 68.
102. *Id.* ¶ 78.
103. *Id.*
104. *Id.* ¶ 28.
105. *Id.* ¶¶ 103–04.
106. Facebook, *supra* note 16, ¶¶ 10, 12.
107. *Id.* ¶¶ 12, 17.
108. *Id.* ¶¶ 13–14.

did Facebook have a responsibility to remove content it was not aware of (i.e., through automatic filtering); second, did Facebook have a responsibility to remove identical or equivalent content posted by any user; and third, did Facebook have a responsibility to remove the content on a global scale?[109]

The CJEU answered in the affirmative to all three questions.[110] While this case was not a typical RTBF case compared to *Google I* and *Google II*, regardless, it was important because it expanded the de-listing of information to social media sites and it applied global injunctions for the removal of information to the automatic filtering of information.[111] The principal outcomes from these three later cases could not only implicate those crucial puzzle pieces of information obtained from OSINT, but it would crucially undervalue OSINT.

C. *The True Value of Open Source Intelligence (OSINT)*

There is no universal definition of OSINT, however, it is statutorily defined by the National Defense Authorization Act of 2006 as "intelligence that is produced from publicly available information and is collected, exploited, and disseminated in a timely manner to an appropriate audience for the purpose of addressing a specific intelligence requirement."[112] One more level of OSINT exists, which is known as validated OSINT—differing from regular OSINT simply by the mere fact that it has a high degree of validity and certainty attached to it.[113]

Historically, OSINT has been around for more than 50 years.[114] Although it has been around for a while, OSINT has always been placed in the backburner due to the IC's belief that its main objective is to "discover and steal secrets" and obtain clandestine information.[115] However, this mindset is flawed. The more technology develops the more it boosts OSINT's credibility and importance.[116] In fact, after World War I, the Office of Strategic Services—the precursor to the CIA created by President Franklin D. Roosevelt—had a branch that would collect newspapers, press clippings or radio broadcasts from around the world to

109. *Id.* ¶ 20.

110. *Id.* ¶ 53.

111. *Id.*

112. National Defense Authorization Act for Fiscal Year 2006, Pub. L. No. 109-63, § 931, 119 Stat. 3136, 3411 (2006).

113. Heather J. Williams & Ilana Blum, *Defining Second Generation Open Source Intelligence (OSINT) for the Defense Enterprise*, RAND CORP. 9 (2018), https://www.rand.org/pubs/research_reports/RR1964.html [https://perma.cc/MCL6-QSNL].

114. RICHARD A. BEST & ALFRED CUMMING, CONG. RSCH. SERV., RL34270, OPEN SOURCE INTELLIGENCE (OSINT): ISSUES FOR CONGRESS 4–5 (2007), https://fas.org/sgp/crs/intel/RL34270.pdf [https://perma.cc/FS8T-TVN5].

115. *Id.*

116. Williams & Blum, *supra* note 113, at 19.

gather intelligence.[117] During the Cold War, the IC would track the published work of scientists and if they discovered a pause, then it would signal that the Russians were developing new technologies.[118]

Some say that OSINT entered a period of dormancy even into the eve of the 9/11 attacks.[119] However, after 9/11, counterintelligence experts began looking at the Internet as a "new frontier" for intelligence gathering. In 2008, a top national security official, Frances Fragos Townsend, noted how the internet and other open source methods of information sharing was the new "battlefield in the war on terror."[120] Some pinpoint the 2009 Iranian "Green Revolution," in which the citizens of Iran were protesting the government regime in power, as the catalyst for the revolutionization of OSINT after its many years of dormancy.[121] The internet suddenly became flooded with Iranian citizen's uploading information related to coordinated political activities, propaganda, and viral content including the protests taking place in Iran, all in almost real-time, and it was all uploaded via the internet and social media.[122] While the protests were unsuccessful, "any individual around the world could mine these social networks for intelligence-grade content, and in the process, write articles, forecasts and deliver insightful intelligence analysis."[123] With the rise of machine learning and the availability of big data coined Web 3.0, it can be said that OSINT has moved into a new phase of collection gathering.[124] Even then, social media has truly been the catalyst for providing a large amount of data and numerous sources to an OSINT analyst's fingertips.

OSIF is split into four categories: (1) widely available data; (2) targeted commercial data; (3) individual experts; and (4) "gray" literature which is made up of writings produced by the private sector, the government, or academia for which access is limited or its existence is not widely known.[125] Examples of sources that fall into the above categories include news articles, academic papers or "computer-based information."[126] About 80% of OSINT is easily accessible information meanwhile 9% is "gray" information and 11% is contested.[127] The way

117. Colquhoun, *supra* note 4.

118. BEST & CUMMING, *supra* note 114, at 4, n.15.

119. *Id.*

120. FRANCES FRAGOS TOWNSEND, REMARKS BY THE ASSISTANT TO THE PRESIDENT FOR THE HOMELAND SECURITY & COUNTERTERRORISM, ODNI OPEN SOURCE CONFERENCE (July 16, 2007).

121. Colquhoun, *supra* note 4.

122. *Id.*

123. *Id.*

124. Williams & Blum, *supra* note 113, at 39.

125. BEST & CUMMING, *supra* note 114, at 6.

126. *Id.*

127. DANIEL LOMAS & CHRISTOPHER J. MURPHY, INTELLIGENCE & ESPIONAGE: SECRETS AND SPIES 24 (2019).

OSINT is defined is important as it determines how its information will be evaluated, treated, and prioritized.[128]

Some argue that OSINT is too narrowly defined.[129] In fact, they propose different definitions all together by eliminating validated OSINT and suggesting to include the term "open-source data," which would be defined as "material . . . of little individual value in isolation but is of intelligence value in compilation" like tweets on views of ISIS within a geographic area or mapping a multitude of IP addresses to create a global picture of internet use in a specific area.[130] Additionally, they consider open source information as more substantive material that can be lawfully obtained through request, purchase, or observation by a member of the public.[131]

These proponents also place open source information into two groups: institutionally generated content and individually generated content.[132] Institutional content consists of news media content and gray literature, meanwhile individual generated content is made up of long-form and short-form social media content.[133] Long-form content is "text-heavy" information obtained from blogs and sites like Reddit.[134] Meanwhile, short-form content is information obtained from sites like Facebook or Twitter.[135] OSINT that is focused on short-form content had little value when observing individual posts on their own; rather, short-form only becomes truly valuable when it is aggregated.[136] For instance, short-form content would become valuable if there are multiple posts from different users in one area where an incident or event is taking place, all giving different accounts of what they see from their different angles and points of view. However, accounts of specific high value interest are the exception to short-form content.[137]

As mentioned before, delineating clear definitions are very important. Until recently, social media was not event considered part of the OSINT definition. In fact, OSINT grouped computer-based information together with media sources. It is important to note that open-source data can include public material that is not explicitly published but is still publicly or commercially available, such as metadata.[138]

---

128. Williams & Blum, *supra* note 113, at 7.
129. *Id.* at 11.
130. *Id.* at 10.
131. *Id.*
132. *Id.* at 11.
133. *Id.*
134. Williams & Blum, *supra* note 113, at 12.
135. *Id.*
136. *Id.*
137. *Id.*
138. *Id.* at 24.

OSINT's expansive amount of information can be its setback too. Only a small portion of large quantities of OSINT information can be utilized and analysts have to sift through a good amount of data.[139] It can be logically argued that this dilution of information and the great efforts it takes to develop OSINT from raw information into actionable intelligence is a reason why OSINT should not be valued as much as other more direct intelligence collection activities.

However, OSINT does contain valuable and beneficial information that can be employed which is why it is important to consider the collection efforts as there is no "clear methodology."[140] Williams & Blum note that there should be four key steps: collection, processing, exploitation, and production.[141] These processes assist in understanding how to effectively acquire, validate, identify the value, and provide the information.[142] An important process to consider is the validation of OSINT, especially as it is applied to information acquired from social media.[143]

It is no surprise that OSINT has become a valuable commodity to intelligence efforts. As Townsend mentioned in her 2008 speech, "much of what is known about our enemies is derived from their own statements, blogs, videos, and chat sessions on the Internet."[144] She notes that the "enemy hides in plain sight."[145] Continuing, she stated "They live and work amongst us, waiting patiently as operational attack plans are developed."[146] OSINT can be a "goldmine of data on public opinion, social networks and interactions, identity and cultural values."[147] In fact, 80% of mission critical information is publicly available.[148] This can be attributed to the fact that there were one billion Internet websites and users in 2008 and 2014 respectively.[149]

---

139. *Id.*

140. *Id.*

141. *Id.* at 13.

142. *Id.*

143. *See id.* at 16–17 (explaining that validation is part of processing, which is important for OSINT since it has an "abundance of available information in a less-structured format").

144. Frances Fragos Townsend, Remarks by the Assistant to the President for the Homeland Security & Counterterrorism, ODNI Open Source Conference (July 16, 2007), https://www.dni.gov/files/documents/Newsroom/Speeches%20and%20Interviews/20070716_speech_2.pdf [https://perma.cc/H3H4-NFKT].

145. *Id.*

146. *Id.*

147. Luke Sloan et al., *Who Tweets? Deriving the Demographic Characteristics of Age, Occupation and Social Class from Twitter User Meta-Data*, PLOS ONE (Mar. 2, 2015), https://journals.plos.org/plosone/article?id=10.1371/journal.pone.0115545#sec001 [https://perma.cc/VS3T-8LWP].

148. Charania, *supra* note 2, at 94.

149. *Id.*

The prevalence of social media has made the Internet an environment rich for intelligence collection. Methods used to collect information from social media have focused on lexical analysis, social media analysis, and geospatial analysis.[150] Lexical analysis shows the most searched-for terms on Google or finds the keywords that have frequently appeared in Internet searches.[151] This type of analysis can also "parse meaning behind language and infer information about the people engaging in social media, including demographic characteristics such as age, social class, economic background and education level."[152]

In social media analysis, the purpose is to analyze the large network of actors rather than the actual individual posting or interacting with the site.[153] Therefore, nodes are utilized to describe individuals outside or inside of a network that help to describe the composition of these networks.[154] Piecing together these nodes allows us to frame together how they interact with each other, what nodes hold more control or power and how they are linked through each other through shared connections.[155] An example of social network analysis is the way that it can help track violent extremist ideology online.[156] Analysts are able to track influencers like ISIS and the way they use social media to propagate language and ideology, while also identifying individuals that may watch an individual YouTube video or read a tweet from followers sharing the same ideology.[157]

Lastly, geospatial analysis consists of geotagging, geolocating, geo-inference, and georeferencing.[158] However, geotagging is probably the most commonly used and known of the four, as this feature is automatically enabled on all cellphones and social media applications and users must be consciously aware to turn such features off if not wanted.[159] Hence, this is why it is known as "volunteered geography" because of its easy accessibility and common use by users.[160] An example of this feature would be the case of the New Zealander Mark Taylor who went to Syria to fight for ISIS and posted approximately 45 tweets with the geotagging feature enabled, which revealed his location, down to the specific house he was residing in, near an ISIS stronghold.[161] Interestingly enough, he

150. Williams & Blum, *supra* note 113, at 23–32.
151. *Id.* at 23–24.
152. *Id.* at 24.
153. *Id.* at 27.
154. *Id*.
155. Williams & Blum, *supra* note 113, at 27–28.
156. *Id.* at 30.
157. *Id.*
158. *Id.* at 31–33.
159. *Id.* at 31.
160. *Id.*
161. Williams & Blum, *supra* note 113, at 32.

attempted to delete, on his own, the 45 geotagged tweets in an attempt to hide where he was located.[162] The most common theme among geospatial analysis is that data obtained from publicly-available information allows certain important targets like geographical markers, specific locations, or even individuals to be located.

The prevalence of social media has proven beneficial to intelligence efforts, while also presenting some challenges. Social media has allowed for easier posting of information for terrorist organizations and its "fan-boys," provides insight on broader goals of terrorist organizations, and gauges public opinion.[163] The proliferation and accessibility of data made available by social media is not unknown to terrorist organizations, however, it is impossible for them to control everything their members do on the Internet.[164] Even with their attempt to control social media activity, many of their members still enable features that allow for their groups to be easily located.[165] But its prevalence has also introduced more noise among valuable information; disinformation; and deception.[166] However, as we will discuss later these factors do not completely devalue the importance and existence of OSINT.

There are three schools of thought surrounding the value of OSINT—those that consider clandestine work as more valuable than OSINT, those that find OSINT valuable and supplemental to clandestine work, and those that are in the middle who do not consider OSINT as the "smoking gun" for certain issues or threats but could help in other ways.[167] Regardless of the school of thought that one may relate to, OSINT is revolutionizing intelligence gathering efforts in its own independent capacity. "OSINT is often underutilized by the IC because of the difficultly in understanding emerging OSINT sources and methods, particularly social media platforms."[168] And while OSINT does provide for an increased amount of data to sift through, advocates of OSINT still propose that its cost is much lower than regular clandestine efforts.[169]

Regardless of the opinions had about OSINT, geographically, it is becoming a key part of intelligence efforts in Canada, the European Union (EU), Asia, and lesser developed countries like Latin America,

---

162. Denver Nicks, *New Zealander ISIS Fighter Accidentally Tweets Secret Location*, TIME (Jan. 1, 2015, 11:08 AM), https://time.com/3651559/new-zealand-isis-twitter/ [https://perma.cc/34RR-H2MH].

163. Charania, *supra* note 2, at 95–97.

164. *Id.* at 95.

165. *Id.*

166. *Id.* at 98.

167. BEST & CUMMING, *supra* note 114, at 2–3.

168. Williams & Blum, *supra* note 113, at 3.

169. Stephen Arnold, *The Other Intelligent Open Source*, 195 INFO. WORLD R. 25 (Oct. 2003).

Africa, and Central Asia.[170] In the EU, Europol and INTCEN have boosted their OSINT operations by budgeting €2.0M on establishing permanent monitoring and reporting of open source information and developing an EC3 platform.[171] In 2016, OSINT investments were calculated as 30% for the Asia-Pacific region; 29% for North America; 23% for Europe; 11% for the Middle East and Africa; and 7% for Latin America.[172] It is forecasted that by 2022 Asia-Pacific will continue to invest the most in OSINT at 32% compared to North America at 27%.[173]

The U.S. is making strides towards investing in OSINT. As a result of the Intelligence and Reform Terrorism Act, the National Open Source Center was created in 2005 within the Office of Director of National Intelligence.[174] In 2015, it was renamed into the Open Source Enterprise and moved to the Central Intelligence Agency as part of the Directorate of Digital Innovation.[175] The National Geospatial-Intelligence Agency (NGA) has advocated that classified sources should supplement public information from open sources.[176] The Defense Intelligence Agency (DIA) has been working on recruiting and hiring data scientists that would focus on OSINT work and the Department of Defense (DOD) established the Defense Open Source Council to support DOD's OSINT initiatives.[177] OSINT will soon be revolutionized by machine learning and automated reasoning.[178] This type of technology will assist in sifting through the extensive amount of data and simplify social media analysis.

OSINT specifically relies on public information taken from websites and search engines, as well as "gray" resources that are not as easily accessible, but public, nonetheless. This can be in the form of metadata and data points populated from social media activities. If the RTBF will be increasingly utilized, especially by social media users, it is possible

170. *Id.*

171. Europol, *Europol Programming Document* 2019-2021, 42, 59, https://www.europol.europa.eu/publications-documents/europol-programming-document [https://perma.cc/JUA3-ZUEX] (last visited Mar. 15, 2021).

172. *Homeland Security Research Corp. (HSRC) Publishes "OSINT Market & Technologies - 2019-2022 Market Report,"* CISION PR NEWSWIRE (June 27, 2019), https://www.prnewswire.com/news-releases/homeland-security-research-corp-hsrc-publishes-osint-market—technologies---2019-2022-market-report-300875282.html [https://perma.cc/PH2N-WP65] (follow the "Open-Source Intelligence Global Market 2019-2022" hyperlink in the first sentence; then scroll down past the "Why Choose Us?" box to the tabbed list reading "Description, Table of Contents, Tables & Figures, More Info"; Under the "Description" tab, scroll down to table labeled "Global Open-Source Intelligence Market Share [%] by Region 2016 & 2022").

173. *Id.*

174. BEST & CUMMING, *supra* note 114, at 11–12.

175. *Id.*

176. Williams & Blum, *supra* note 113, at 37.

177. *Id.* at 39.

178. *Id.*

that targets of OSINT may want to remove themselves or traces of their activities that might assist in intelligence gathering efforts.

D. *The Intersection of RTBF and OSINT*

As we have seen from the RTBF case law, the conversation centers around removing public information contained in search engine results, webpages or social media posts. This information is the building blocks of OSINT. The thesis of this Article assumes that first, the requesters are aware of the RTBF process and are knowledgeable of how to request this process. The second assumption is that the RTBF process is not a lengthy one. If the opposite were true, then taking advantage of such process would not be as beneficial to those requesters that are avoiding OSINT sweeps. The third is that there is no trust deficit among groups or individuals that would be subjects of interest for OSINT sweeps. Without trust deficits, there is a higher reliance on technology by these parties.[179]

The claims proposed above are more than plausible. Potential targets, especially terrorist organizations are very knowledgeable and involved in social media culture. In 2015, there was almost 18,000 accounts related to ISIS and similar groups including Al Qaeda use "bots" to broadcast their cause.[180] ISIS and its supporters also utilize encrypted platforms like Telegram to communicate with each other.[181]

The RTBF precedent promotes a swift process from the time a request is made to an electronic communication service provider and de-list or de-referencing occurs. In 2015, after the *Google v. Spain* decision, Google received more than 254,000 removal requests from countries across Europe.[182] The requests came from the following top four countries: U.K., Germany, France, and the Netherlands.[183] Seventy percent of RTBF requests were being denied by Google.[184] The timing it took for Google to process these requests was about 16 days.[185] Between May 2014 and February 2018, it received over 2.4 million requests, but only 43% have been approved.[186]

---

179. *See* Zeeshan-Ul-Hassan Usmani, *Predictive Modeling to Counter Terrorist Attacks*, 20 BROWN J. OF WORLD AFFS. 277, 281 (2014) (explaining that terrorist organizations do correlate data with each other, especially attacks).

180. Charania, *supra* note 2, at 98.

181. *Id.*

182. Greg Sterling, *Google Offers Insight Into Its Right-to-be-Forgotten Review Process*, MKTG. LAND (May 13, 2015, 4:54 PM), https://marketingland.com/we-vote-google-offers-insight-into-its-right-to-be-forgotten-review-process-128686 [https://perma.cc/X2P5-KK36].

183. *Id.*

184. *Id.*

185. *Id.*

186. Paul Sawers, *Google Has Received 2.4 Million 'Right to be Forgotten' URL Delisting Requests and Fulfilled 43%*, VENTURE BEAT (Feb. 27, 2018, 2:27 AM), https://venturebeat.com

The fact that the GDPR has only been in effect for five years could signal a continued increase in these requests. It is also well-known that terrorist organizations do speak and work with each other.[187] There is no trust deficit between terrorist groups.[188] The fact that there is a lack of coordination between agencies within the same country or extraterritorially could be the reasons why groups may be one coordinated attack ahead of counterterrorism efforts.[189] These explained assumptions only prove that our discussion about OSINT and the unintended consequence of the RTBF is not far-fetched.

With its extraterritorial application, almost all technology companies would be subject to GDPR regulation, so long as they process the data of an EU resident. For example, on Twitter's website, it explains how they are considered data controllers in some situations, but data processors in others.[190] The GDPR broadly defines data, therefore, it would be neglectful to believe that only web searches, as the ones discussed in the *Google* cases, would apply to the RTBF. In fact, some agree that the RTBF's reach will expand to other types of crucial data, such as "the metadata, conversations and media shared in direct messages between users, device tokens, email and phone number contact lists, IP address audits, and [] inferred data like user, age, gender, languages spoken, and interests."[191] The fact that most of this information is available through host sites[192] or social media applications like Twitter and Facebook—is even more troubling, considering that in the *Facebook* case the CJEU determined that Facebook was a data controller under the GDPR.[193] It also obligated these sites to remove posts and comments that were not only identical, but of "equivalent content" that is deemed illegal.[194] These actions would apply globally through automatic filters.[195]

This precedent is extremely expansive. Scholars argue that the RTBF precedent has created "an unprecedented imbalance in the Internet ecosystem in favor of data subjects' erasure requests" over those of the

/2018/02/27/google-has-received-2-4-million-right-to-be-forgotten-url-delisting-requests-and-fulfilled-43 [https://perma.cc/C4QE-2K9N] .

187. Usmani, *supra* note 179, at 280–81.

188. *Id.*

189. *Id.*

190. *Twitter for Business FAQ 3*, TWITTER, https://gdpr.twitter.com/en/faq.html [https://perma.cc/ED7K-LFT9] (last visited Nov. 3, 2020).

191. Johnson, *supra* note 21.

192. Host sites are defined as online service providers that "store content uploaded by users, typically making it accessible to other people online." Keller, *supra* note 48, at 322–23.

193. Keller, *supra* note 48, at 323 (citing *CG v. Facebook Ireland Ltd* [2016] NICA 54, ¶¶ 88, 91 (Nor. Ir.), http://www.bailii.org/nie/cases/NICA/2016/54.html).

194. Facebook, *supra* note 16, ¶¶ 45–46.

195. *Id.*

data controllers.[196] Not only has RTBF placed an obligation on online internet and social media platforms (technology platforms) to determine answers to legal questions that could vary from country to country, but this imbalance has been fueled by huge fines, bad press or damaged relationships with DPA's. Most arguments center on the fact that it could prove negatively for freedom of expression, but the same could be said for intelligence efforts. Ultimately, this will lead to technology platforms "honor[ing] not only legitimate RTBF requests but also mistaken or abusive ones."[197] It has also been proven that platforms "comply with legally baseless requests all too often."[198]

Google has already received requests from individuals asking to remove information related to public officials, priests and professionals attempting to hide criminal and unsavory acts.[199] Additionally, 90% of the requests received consists of delisting personal information.[200] One request from an individual sought to delist one URL on the website of a government department, which included information on the individual's affiliations with a terrorist organization.[201] Luckily, Google did not delist the URL.[202] Delisting or removing any information from search results is not an inconsequential issue but removing information from host sites can be much more harmful.[203] The information is removed from the Internet completely and the author's only copy would be eliminated.[204] While this could prove detrimental for author expression, it is much more unfavorable for OSINT efforts that rely on the now-deleted information.[205]

We have seen how OSINT proves beneficial for intelligence gathering. It allows us to analyze terrorism recruitment efforts, locations, and behaviors. However, there are some concerning attributes. With so many privacy features or encryption applications, can we effectively track online activity? Terrorist groups are more than aware of their digital footprint and attempt to be as careful as possible. Also, while most of us strive to place as many privacy settings on our data, not everything on the

196. Dawn C. Nunziato, *The Fourth Year of Forgetting: The Troubling Expansion of the Right to be Forgotten*, 39 U. Pa. J. INT'L L. 1011, 1056 (2018).

197. Keller, *supra* note 48, at 291.

198. *Id.*

199. *Id.*

200. *Requests to Delist Content Under European Privacy Law*, GOOGLE, https://transparencyreport.google.com/eu-privacy/overview [https://perma.cc/6JTA-9ZU3] (last visited Nov. 3, 2020).

201. *Id.*

202. *Id.*

203. Keller, *supra* note 48, at 325.

204. *Id.*

205. *Id.*

internet is private. To err is to be human, but it is OSINT's job to monopolize on those errors and "privacy loopholes."

One major issue is whether the information obtained is reliable or not. On the internet, anyone can pose as anyone or post anything without credibility. Some argue that having to continue confirming reliability of OSINT is costly and timely, but even with clandestine information, there is always a level of authentication that is required. Falsification and disinformation do not discontinue OSINT's value and instead, it is RTBF's rising precedent that could play a part in minimizing and devaluing its worth. Factors like falsification and expansive data are issues that have solutions. Terrorist groups will always be on the internet, especially for recruitment purposes, therefore, they will co-exist in the virtual world leaving some footprints or evidence behind. Meanwhile, mining through troves of data will be possible through better and more developed OSINT technology, especially machine learning capability software. However, removing data is consequential and irreplaceable. Once the evidence is destroyed, it is no longer accessible.

II. SOLUTIONS

OSINT, for purposes of national security, is valuable and important, but protecting the privacy and civil liberties of individuals is just as crucial. While the majority of information that would be implicated by this Article's discussion centers around foreign targets, specifically those residing in the EU or communicating with individuals in the EU, it is prudent to point out that there is always the highest probability that the information of U.S. persons—a citizen or permanent resident—may be implicated. This scenario is most probable when it comes to acquiring social media information. The IC must be mindful of this implication and it must always ask itself the following questions: What is the information obtained? How will the information be utilized? What proper laws could be applicable to the use of the information? Executive Order 12333 does outline the procedures that must be followed to collect and retain the information of U.S. persons.

When it comes to EU persons, the GDPR serves to protect and preserve the individual privacy of its individuals. The RTBF model is an outgrowth of the importance by EU law to create choices for individuals by allowing them to decide what level of privacy they deem important. When an individual submits an RTBF request, they are choosing to exercise a level of privacy on their information. It is unimaginable to argue that privacy is not an important right that must be preserved. Instead, this Article seeks to argue that privacy should be understood and

defined from a pluralistic perspective.[206] By understanding privacy from this approach, you can attempt to analyze the specific issues of privacy that evolve around specific sets of problems.[207]

The concept of privacy should not be antiquated nor disregarded. Instead, it should be upgraded. It should be regarded as consisting of more than just one single concept. In the surveillance context, I propose that we think about privacy in the context of digital privacy versus individual self-privacy. What you are able to allow to "commodize" about yourself (i.e. what is allowable by you to make publicly available by self-control) is your digital privacy. Your individual self-privacy is what occurs in the kinetic world that you understand to be subject to an absolute form of privacy. Former ODNI General Counsel, Robert S. Litt stated in his speech:

> Why is it that people are willing to expose large quantities of information to private parties but don't want the Government to have the same information? Why, for example, don't we care if the telephone company keeps records of all of our phone calls on its servers, but we feel very differently about the prospect of the same information being on NSA servers? This does not seem to me to be a difficult question: we care because of what the Government could do with the information.[208]

In fact, I believe that in the privacy context, we are more worried with who has our data than what it is done with it.[209] Therefore, the privacy issue should rest more on self-control of the individual than of a blanket dismissal of government practices. But, to live up to this privacy model, it is also up to the government to foster and build up that trust.

This leads to the distrust. The RTBF precedent is a logical outgrowth of an insecurity shared by citizens that was created by the actions of governments and technology companies. Oddly enough, the RTBF legal model rests much of the decision power to technology platform's, who determine the extent of what content to remove and why. It is up to

206. Daniel J. Solove, *'I've Got Nothing to Hide' and Other Misunderstandings of Privacy*, 44 SAN DIEGO L. REV. 745, 756 (2007).

207. *Id.*

208. Robert S. Litt, *Privacy, Technology, and National Security: An Overview of Intelligence Collection*, OFF. DIR. NAT. INTEL. (Nov. 21, 2020, 9:46 PM), https://www.dni.gov/index.php/newsroom/speeches-interviews/speeches-interviews-2013/item/896-privacy-technology-and-national-security-an-overview-of-intelligence-collection-by-robert-s-litt-odni-general-counsel#:~:text=Why%20is%20it%20that%20people,to%20have%20the%20same%20information%3F&text=entirely%20understandable%20concern%20that%20the%20Government%20may%20abuse%20this%20power [https://perma.cc/FFP7-7SYN].

209. *See* Steven C. Bennett, *The "Right to be Forgotten": Reconciling EU and US Perspectives*, 30 BERKELEY J. INT'L L. 161, 165 (2012) (explaining suggestions for ways to approach this area by looking at "source of the content" rather than where the content is shared).

governments to reinstate confidence in their intelligence efforts and privacy responsibilities.

To ease the consequences of RTBF, there must be compromise. To achieve this compromise, the U.S. could enter into data agreements with EU member states, similar to the U.S. and U.K. agreement that resulted from the CLOUD Act passed by Congress in 2019.[210] By entering into agreements, it could assist with bridging the differences in law, especially with regard to privacy.[211] If no agreement is entered into, then the U.S. cannot acquire, process or retain the data of any foreign target from that EU member state.[212] As illustrated by David Luban, *et al.*, the result "of an interconnected world . . . is a clear trend towards . . . convergence among the various legal systems around the world" and therefore "traditions are eroding."[213] Therefore, new approaches need to be considered, especially with our advanced state of technology within society.

In the *Facebook* case, the CJEU emphasized the disparity in member states' legislation and case law "concerning liability of service providers acting as intermediaries [which] prevent the smooth functioning of the internal market . . . by impairing the development of cross-border services . . . ."[214] If that is so, then the CJEU would likely agree that agreements like this would provide an ample solution to prevent further disparities by addressing how these providers should treat the data of individuals.

The CLOUD Act stemmed from an inconsistency in U.S. law regarding the extraterritoriality of the Electronic Communications Provider Act, which regulated data transfers of technology companies and their cooperation with law enforcement.[215] Currently, countries can request information needed for law enforcement investigations through the Mutual Legal Assistance Treaty (MLAT) process, which can be a long, arduous, frustrating procedure.[216] MLAT is rooted in international law, which allows for the creation of "bilateral and regional treaties governing both U.S. law enforcement's acquisition of user data from foreign jurisdictions and vice-versa."[217] It would set expectations on evidence gathering, law enforcement behaviors, and any other treaty-related cooperation activity.[218]

---

210. Consolidated Appropriations Act of 2018, P.L. 115-141, 132 Stat. 348 [CLOUD Act].

211. *Id.* at 193.

212. Brehmer, *supra* note 31, at 937.

213. DAVID LUBAN ET AL., INTERNATIONAL AND TRANSNATIONAL CRIMINAL LAW 135 (3d ed. 2018).

214. Facebook, *supra* note 16, at ¶ 40.

215. Brehmer, *supra* note 31, at 934, 940, 954.

216. *Id.* at 950–51.

217. *Id.* at 950.

218. *Id.* at 950–51.

However, these MLATs can take many years to be finalized and not all participating states have a fully-staffed or existing Central Authority that could assist in the creation of these agreements. By the time an agreement is finalized, it is too late to obtain important evidence. Enter the CLOUD Act, which sets aside the legal barriers to allow access to electronic data from other countries for purposes of criminal investigations.[219] Ultimately, it allows the executive branch to enter into agreements, which "determine which countries qualify based on several factors, including whether the foreign country has entered into an appropriate executive agreement, and whether the foreign country 'affords robust substantive and procedural protections for privacy and civil liberties in light of the data collection . . . .'"[220]

In *Google I*, the CJEU left open the possibility for EU member states to consider whether they would apply RTBF provisions extraterritorially.[221] With this precedent, it would not be unusual for member states to enter into agreements that would assist U.S. intelligence efforts while still incorporating civil liberty protections and privacy rights for EU persons. In other CJEU case law, the U.S. has already conceded to greater data transfer restrictions than its EU counterparts such as in the *Max Schrems v. Data Protection Commissioner* case and other reported comparisons.[222] The U.S. has displayed a willingness to come to the table and agree on these important issues and concede on areas when necessary. Although it would not be fair for the U.S. to be treated similarly as other EU counterparts, especially when it comes to its own laws and regulations on intelligence.

The GDPR allows its member states to exercise derogations in certain sections.[223] As a result of these derogations, data controllers and processors must consider member states' own national laws, in addition to other provisions of the GDPR and CJEU case law.[224] As it stands, the U.K. has derogated from Article 17 RTBF provisions by being one of the first countries to establish an agreement with the U.S. under the CLOUD Act model.[225] This proves that countries are willing to come to a consensus under a bilateral agreement, and those bilateral agreements

219. *U.S. and U.K. Agreement*, *supra* note 23.

220. *U.S. Cybersecurity and Data Privacy Outlook*, GIBSON DUNN (Jan. 28, 2019), https://www.gibsondunn.com/us-cybersecurity-and-data-privacy-outlook-and-review-2019/ [https://perma.cc/Q4LG-5KBE].

221. Google I, *supra* note 14, ¶ 72.

222. Brehmer, *supra* note 31, at 958; *See also* Christopher Wolf & Winston Maxwell, *Why the U.S. is Held to a Higher Data Protection Standard*, IAPP (May 2, 2015), https://iapp.org/news/a/why-the-u-s-is-held-to-a-higher-data-protection-standard-than-france/ [https://perma.cc/DCG2-DWNL].

223. GDPR, *supra* note 10, art. 49.

224. GDPR, *supra* note 10, arts. 85, 89.

225. *U.S. and U.K. Agreement*, *supra* note 23.

could be a solution to addressing the differences in how privacy is perceived among the various countries. This particular solution could also help define what truly is a national security exemption. There should be no reason that this bilateral agreement solution would contradict the GDPR seeing as Recital 16 of the GDPR allows for member states to execute actions for national security interests separate from the GDPR.[226]

It is imperative that "national security" be both exercisable and properly defined under Article 23 of the GDPR.[227] By agreeing on a proper definition, it would allow for EU member states to work with the U.S. to derogate from aspects of the GDPR, especially RTBF, during the processing of OSINT information of EU persons for national security issues.

The Working Party attempted to dissect the issues surrounding the national security exemption and found concerns regarding U.S. surveillance. I discussed above how the national security exemption is comprised of three situational contexts that would need to be addressed.[228] By properly establishing an agreed upon definition, whether to be applicable across the entire EU or with each member state, it would allow for the proper derogation without the negative stigma surrounding U.S. surveillance. While case law is scarce on this issue, the definition could consider factors such as the individual involved and their location or citizenship status; requiring a set of articulable facts similar to the Fourth Amendment search warrant model; and setting a mandatory time limit of data processing and retention of 30 days with a follow-up review by the proposed oversight committee.

The oversight mechanism of RTBF is not balanced, especially for certain types of technology.[229] The GDPR created the DPA role, which is appointed by each EU member state.[230] The role was created through Directive 95/46/EC[231] and strengthened by the GDPR.[232] All DPA's consist of independent organizations, who have a number of responsibilities as dictated under Article 57 of the GDPR.[233] Their main purpose is to protect fundamental rights and freedoms of natural persons with relations to data processing and the facilitation of the free flow of data.[234]

Although the DPA role requires impartiality as directed by Article 52

---

226. *Recital 16*, *supra* note 75.

227. GDPR, *supra* note 10, art. 23.

228. *See* Part I. B.

229. *See* Keller, *supra* note 48, at 318, 338 (discussing the framework of RTBF claims as it applies to host sites).

230. GDPR, *supra* note 10, art. 51.

231. Hoofnagle, *supra* note 34, at 94.

232. Keller, *supra* note 48, at 316-17.

233. GDPR, *supra note* 10, art. 57; Hoofnagle, *supra* note 34, at 96.

234. Keller, *supra* note 48, at 357.

of the GDPR, some have observed that the DPA model has lacked "adequate independence."[235] As Keller argues, DPA's have an interest in making sure that host sites are obligated under RTBF to increase their effective authority.[236] The review of RTBF requests are also swayed in favor of privacy.[237] This is due to the lack of public review of DPA decisions.[238] If there is a disagreement between the DPA and the technology platforms, there is no intermediary to assist with the disagreement other than the CJEU.

While the DPA model was created to monitor data controllers and processors, it would be much more helpful to create a separate and independent data monitoring committee, similar to the composition of the Global Internet Forum to Counter Terrorism (GIFCT) and the similar objectives of the Interpol. The GIFCT was created by a group of technology companies who wanted to share best practices on addressing terrorism abuse on their platforms.[239] Recently, they announced that they would be transforming GIFCT into an independent body with its own Executive Director.[240]

The overall goal of GIFCT was to provide a space for sharing of knowledge on this one narrow issue of terrorism, while also providing incident protocol and joint technology innovation.[241] With my proposed committee, the primary focus would be somewhat similar to GIFCT. It would be a space to create information-sharing protocols that would adhere and address all EU member states' concerns. This committee would serve as a neutral organization that would assist with managing data transfers.

The Interpol model provides the same level of information-sharing. Instead, the Interpol works with countries and serves as a sounding board for transnational criminal law. This proposed committee would be comprised of experts in the national security and privacy field that would be privy to sensitive, classified information. This committee could also serve as the Central Authority for the bilateral agreements discussed above. The current Data Protection Board is charged with enacting policy and best practices as it relates to the entire GDPR. However, the proposed

---

235. Hoofnagle, *supra* note 34, at 94.

236. Keller, *supra* note 48, at 338.

237. *See Id.* at 321 (determining that there are incentives for online service providers to err on the side of the data subject's rights for fear of facing large fines from the GDPR).

238. *Id.* at 356; *See* Nunziato, *supra* note 196, at 1044 (noting the lack of notice and opportunity to be heard for whom erasure is directed at from the RTBF provision).

239. GLOB. INTERNET F. TO COUNTER TERRORISM, https://gifct.org/about/ [https://perma.cc/8TRY-4GEU] (last visited Mar. 15, 2021).

240. *Progress for the Independent GIFCT*, GLOB. INTERNET F. TO COUNTER TERRORISM (Dec. 11, 2019), https://gifct.org/press/progress-independent-gifct/ [https://perma.cc/S8CU-KV94].

241. GLOB. INTERNET F. TO COUNTER TERRORISM, *supra* note 239.

committee would focus on the intricate and nuanced process of data transfers and information sharing for purposes of national security issues.

CONCLUSION

When the ECJ ruled in favor of erasure in *Google v. Spain*, it was not apparent how this one decision would start a series of other actions and decisions that would promote unintended consequences in the area of data and intelligence gathering. While the GDPR has only been in effect for a few years, it seems that it is here to stay. Therefore, with a focus on cooperation and a different approach to privacy enforcement, there can be some medium that could appease both sides of the debate. In the five years that RTBF has been in existence, countries outside of the EU like Colombia, Japan, Mexico, and Russia have been recognizing and incorporating the RTBF model.[242] In fact, most adopted laws within months of the *Google v. Spain* decision.[243] With the globalization of RTBF, it is imperative that we continue to have productive discussions on this topic.

242. Nunziato, *supra* note 196, at 1059–63.
243. *Id.*