Indiana Int'l & Comp. Law Review

Volume 30 Number 1 2019

NOTE

MAJOR FLAWS IN MINOR LAWS: IMPROVING DATA PRIVACY RIGHTS AND PROTECTIONS FOR CHILDREN UNDER THE GDPR

VIRGINIA A. M. TALLEY*

INTRODUCTION

The world of big data and technology is advancing at a rapid rate.[1] For example, in 1984 Motorola introduced the first hand-portable cellular phone to the public market, costing nearly $4,000 (equivalent to over $9,000 today) and weighing just under two pounds.[2] Thirty years ago, the flip phone design was introduced and quickly became an international symbol of status as the first pocket sized personal communication device.[3] Today, just twelve years after the introduction of the first Apple iPhone by Steve Jobs on the MacWorld Convention stage, "screen time" is so common amongst the population that groups like the Centers for Disease Control and the American Academy of Pediatrics have published guidelines for how much "screen time" is appropriate and healthy for the younger populations.[4]

---

* Virginia A. M. Talley, J.D., 2020 (expected) Indiana University Robert H. McKinney School of Law; B.A. Political Science, B.A. Sociology, 2016 Indiana University. The author thanks her family and friends for their constant support, the Indiana International & Comparative Law Review for their invaluable efforts in bringing this Note to publication, and Professors James Nehf and Meaghan Zore, and other mentors for encouraging her interest in data privacy and the law.

1. Simone van der Hof, *Article: I agree… or do I? – A Rights-Based Analysis of the Law on Children's Consent in the Digital World*, 34 Wis. Int'l L.J. 409, 412, 414 (2016).

2. Pagan Kennedy, *Who Made that Cellphone?* THE NEW YORK TIMES (Mar. 15, 2013), https://www.nytimes.com/2013/03/17/magazine/who-made-that-cellphone.html [https://perma.cc/AFY4-EY7G]. *See also* Justin Meyers, *Watch the Incredible 70-Year Evolution Of the Cell Phone*, BUSINESS INSIDER (May 6, 2011), https://www.businessinsider.com/complete-visual-history-of-cell-phones-2011-5 [https://perma.cc/5RZC-WUMQ].

3. Meyers, *supra* note 2. *See also* Mark Hall, Motorola, Inc.: American Company, BRITANNICA (January 19, 2019), https://www.britannica.com/topic/Motorola-Inc#ref1078869.

4. *The History of the iPhone: 2007-2019*, The History Cooperative, (Jan.19, 2019), https://historycooperative.org/the-history-of-the-iphone/ [https://perma.cc/Z9SG-Y5KK]. *See also Screen Time v. Lean Time Infographic*, Centers for Disease Control and Prevention (Mar. 13, 2017), https://www.cdc.gov/nccdphp/dch/multimedia/infographics/getmoving.ht [https://perma.cc/37N4-LVG9]. *See also Children and Media Tips from the American Academy of*

Studies estimate that 170,000 children go online for the first time every day.[5] For many people in modern society, technology and the Internet are increasingly prominent parts of daily lives, especially among the younger populations.[6] In 2017, an estimated forty percent or more of children in the United States had their own tablet device.[7] This number was a dramatic increase from the less than one percent of children who owned a similar device in 2011.[8] Children are now "growing up digital" and using personal devices to consume media and get connected to the world wide web, and it is of growing concern to ensure children are adequately protected online.[9]

Privacy is a growing concern, too, as people become more aware and more protective of the ways in which their personal data are collected and used.[10] Most adults in the Internet age have some idea of the extent to which their data is collected, stored, and analyzed, whether for targeted marketing, automated profiling, or some other purpose.[11] Many are concerned with the inability to control the ways in which their personal information is processed, and new privacy frameworks allow individuals to take better control over how their personal data is collected and used.[12]

Parents are also increasingly concerned about their children's online activities as well as the companies collecting information regarding those activities.[13] New

---

Pediatrics, American Academy of Pediatrics (May 1, 2018), https://www.aap.org/en-us/about-the-aap/aap-press-room/news-features-and-safety-tips/Pages/Children-and-Media-Tips.aspx [https://perma.cc/F3T5-GWHY].

5. Angus Chen, *UNICEF Is Unhappy About Lack of Online Protection For Kids*, NPR: NATIONAL PUBLIC RADIO (Dec. 22, 2017), https://www.npr.org/sections/goatsandsoda/2017/12/22/571709062/everyday,%20according%20to%20a%20new%20UNICEF%20report [https://perma.cc/ZG7R-KJM2]. *See also* Sara Fischer, *The Internet reckons with Kids*, AXIOS (Dec. 4, 2018), https://www.axios.com/internet-kids-online-privacy-oath-payout-29b6a61c-637e-4650-afb5-a56da099e39b.html [https://perma.cc/3EUB-4BCK].

6. *Children and the Internet*, INTERNET SOCIETY (Nov. 23, 2018), https://www.internetsociety.org/resources/doc/2012/children-and-the-internet/ [https://perma.cc/9PJG-PXDW].

7. *The Common Sense Census: Media Use by Kids Age Zero to Eight*, COMMON SENSE MEDIA (2017) at 36, https://www.commonsensemedia.org/sites/default/files/uploads/research/csm_zerotoeight_fullreport_release_2.pdf [https://perma.cc/95ZY-QDXX].

8. *Id*.

9. *Children and Media Tips from the American Academy of Pediatrics, supra* note 4. *See also Children and Parents: Media Use and Attitudes Report*, OFCOM: MAKING COMMUNICATIONS WORK FOR EVERYONE (Nov. 29, 2017), at 5, 15, https://www.ofcom.org.uk/__data/assets/pdf_file/0020/108182/children-parents-media-use-attitudes-2017.pdf [https://perma.cc/YSR4-PC6D].

10. van der Hof, *supra* note 1 at 444, 445.

11. *In re* Nickelodean Consumer Privacy Litig., 827 F.3d 262, 266 (2016).

12. *Completing a trusted Digital Single Market for all The European Commission's contribution to the Informal EU Leaders' meeting on data protection and the Digital Single Market in Sofia*, at 3, COM (2018) 320 final (May 16, 2018). (Two-thirds of Europeans say that they are worried about having no control over the information they provide online . . .").

13. *Children and Parents: Media Use and Attitudes Report*, *supra* note 9.

regulations are supporting more robust privacy rights for individuals, including stronger transparency and consent requirements, as well as new rights to access and erasure of information.[14] Children have a right to these privacy protections as well.[15]

The United Nations Convention of the Rights of the Child provides that, "no child shall be subjected to arbitrary or unlawful interference with his or her privacy, family, home or correspondence, nor to unlawful attacks on his or her honour and reputation."[16] As such, protecting children, their personal data and their right to privacy becomes increasingly important as the presence of minors on the Internet continues to increase.[17]

A 2011 "State of the Net" survey conducted by *Consumer Reports* showed that of the twenty million minors that used the popular social media site Facebook, 7.5 million of them were younger than age thirteen.[18] According to the E.U. Kids Online project, a survey conducted in 2011 indicated that 59% of children between ages nine and sixteen had social media profiles.[19]

When it comes to providing consent for various data tracking applications and websites, many children, and many adults, for that matter, do not thoroughly understand the extent to which their data is being collected, used, or processed.[20] The majority of people, when presented with a lengthy, small-print pop-up about

---

14. *Completing a trusted Digital Single Market for all The European Commission's contribution to the Informal EU Leaders' meeting on data protection and the Digital Single Market in Sofia*, *supra* note 12.

15. Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools)*, 398/09/EN at 3 (Feb. 11, 2009), https://www.garanteprivacy.it/documents/10160/10704/1619292 [https://perma.cc/MWA4-S73H].

16. *Convention on the Rights of the Child,* Nov. 20, 1989, 1577 U.N.T.S. 3, art. 16 § 1. *See also* Article 29 Data Protection Working Party, *Opinion 2/2009 on the protection of children's personal data (General Guidelines and the special case of schools),* 398/09/EN at 3 (Feb. 11, 2009), https://www.garanteprivacy.it/documents/10160/10704/1619292 [https://perma.cc/MWA4-S73H].

17. Milda Macenaite & Eleni Kosta, *Consent for processing children's personal data in the EU: following in US footsteps?* (2017), 26 INFORMATION & COMMUNICATIONS TECHNOLOGY LAW 146, 147-48.

18. *CR Survey: 7.5 Million Facebook Users are Under the Age of 13, Violating the Site's Terms,* CONSUMER REPORTS (Nov. 24, 2018), https://www.consumerreports.org/media-room/press-releases/2011/05/cr-survey-75-million-facebook-users-are-under-the-age-of-13-violating-the-sites-terms-/ [https://perma.cc/G5ZU-H2TB].

19. Sonia Livingstone et al., *Risks and safety on the Internet: The perspective of European children*, THE LONDON SCHOOL OF ECONOMICS AND POLITICAL SCIENCE (2011), http://www.lse.ac.uk/media%40lse/research/EUKidsOnline/EU%20Kids%20II%20(2009-11)/EUKidsOnlineIIReports/D4FullFindings.pdf [https://perma.cc/BE4Q-P2WF]. *See also* Custers et al., *Informed Consent in Social Media Use – The Gap Between User Expectations and EU Personal Data Protection Law*, 10 SCRIPTED 4, 435-39 (2013).

20. van der Hof, *supra* note 1, at 437-38.

privacy policies or user agreements, do not take the time to read the agreement, let alone to understand the agreement, as the agreement is often information overload and the user does not have meaningful choice in the matter.[21] This commonly occurring, seemingly insignificant disregard for the data rights and protections of the consenter raises a number of issues in regard to current consent models and data protection frameworks in the United States and European Union.[22]

For processing the personal data of children, however, the E.U.'s new General Data Protection Regulation (the "GDPR" or "Regulation") provides a framework for obtaining proper consent to collect and use children's data.[23] The preceding data protection framework, the Data Protection Directive (the "Directive"), did not contain specific provisions regarding the privacy rights or data protections for children, but instead applied the Directive's provisions to children as individuals in their own right.[24] While the GDPR has taken steps toward more strongly protecting children in the Internet age, the provisions for protecting children's personal data in the E.U. face challenges ahead.[25] The child-specific protection laws under the GDPR in the E.U. are inspired by the United States' Children Online Privacy Protection Act, which has faced its own challenges in its almost two decades of implementation in the U.S.[26] The challenges, however, provide a perspective from which improvements to the European data protection framework can be derived, especially regarding the protection of children's personal data.[27]

The purpose of this Note is to examine the current state of laws for processing the personal data of children in the European Union and United States. After discussing the General Data Protection Regulation and its measures to protect the personal data of children, it will compare the Regulation with the Children's Online Privacy and Protection Act as currently implemented and enforced in the United States. The GDPR has enacted special protections for children's data, among a long list of newly delineated rights and protections, and this Note will discuss the ways in which the developing framework of the GDPR could strengthen its provisions to better protect children, their data and their rights to privacy.

This Note will address the processing of children's personal data under the lawful basis of consent. While the GDPR allows data processing for other purposes, this Note addresses the ways in which processing children's personal data under the lawful basis of consent is inadequate as currently enumerated in

---

21. Dr. Bart W. Schermer et al., *The Crisis of Consent: How Stronger Legal Protection may lead to Weaker Consent in Data Protection*, ETHICS & INFORMATION TECHNOLOGY, 17 (Feb. 25, 2014).

22. *Id*.

23. van der Hof, *supra* note 1, at 424.

24. *Id*.

25. van der Hof, supra note 1, at 437-38.

26. Macenaite & Kosta, *supra* note 17, at 148.

27. Macenaite & Kosta, *supra* note 17, at 191.

the Regulation. Part II of this Note discusses the history and development of data protection, privacy frameworks, and children's privacy law in the European Union. Part III provides a background of data privacy laws and children's privacy protections in the United States. Part IV analyzes the current regulations for processing the personal data of children in the E.U. and discusses the successes and setbacks children protection laws have experienced in the United States. This section also identifies areas in which the GDPR could improve to provide stronger protections when processing the personal data of by comparing the E.U. legislation to the child privacy laws in the United States. Following the comparison and analysis of the relevant consent regulations, Part V concludes the note by suggesting potential amendments that could strengthen the protective measures currently in place for children and their data under the European Union's GDPR.

II. HISTORY OF DATA PRIVACY AND CURRENT CHILD PRIVACY LAWS IN THE E.U.

A. History of Data Privacy in the E.U.

One of the European Union's first major moves toward data protection was adopted in 1995, and known as Directive 95/46/EC, or more commonly, the Data Protection Directive ("Directive").[28] The Data Protection Directive regulated the collection and processing of personal data within the European Union and applied to all Member States.[29] This directive was constructed from the principles laid out in the Organisation for Economic Co-operation and Development's ("OECD") Guidelines on the Protection of Privacy and Transborder Flows of Personal Data first adopted in 1980.[30]

The OECD's Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, and therefore the Data Protection Directive, aimed to protect personal data and the fundamental human right of privacy.[31] The Guidelines on the Protection of Privacy and Transborder Flows of Personal Data set out eight Mandatory Data Protection Principles, seven of which served as a framework for both the Data Protection Directive, and later the General Data Protection

---

28. Nate Lord, *Data Protection 101: What is the Data Protection Directive? The Predecessor to the GDPR,* DIGITAL GUARDIAN (Sept. 12, 2018), https://digitalguardian.com/blog/what-data-protection-directive-predecessor-gdpr [https://perma.cc/U777-N6U9].

29. *Id*.

30. *OECD Guidelines on the Protection of Privacy and Transborder Flows of Personal Data*, ORGANISATION FOR ECONOMIC CO-OPERATION AND DEVELOPMENT (Oct. 10, 2018), http://www.oecd.org/sti/ieconomy/oecdguidelinesontheprotectionofprivacyandtransborderflowsofpersonaldata.htm [https://perma.cc/DDS4-LMVZ].

31. *How did we get here? An overview of important regulatory events leading up to the GDPR*, EUGDPR.ORG (Oct. 10, 2018), https://eugdpr.org/the-process/how-did-we-get-here/ [https://perma.cc/P8GP-8U6H].

Regulation.[32] The General Data Protection Regulation sets out these seven key principles which serve, along with their compliance, as the fundamental building blocks for the GDPR are strong data protection practices.[33] The seven principles of data protection in the GDPR are: (1) lawfulness, fairness and transparency; (2) purpose limitation; (3) data minimization; (4) accuracy; (5) storage limitation; (6) integrity and confidentiality; and (7) accountability.[34]

The Data Protection Directive was designed as a data protection goal that European Union countries must achieve, although the means by which the goal was achieved was left to be decided by the individual countries.[35] European Union directives lay out guidelines which each Member State interprets into its own law.[36] The Data Protection Directive, by nature, resulted in varied interpretations of the data privacy guidelines in the form of national data privacy law.[37]

While the Directive held true to the original recommendations of the OECD and the concepts of the fundamental human right to privacy, the quickly evolving technological and data-driven environment called for an updated and more enforceable set of regulations to protect personal data and privacy rights of E.U. data subjects.[38] This need manifested in the form of the General Data Protection Regulation, which, as a regulation rather than a directive, is an enforceable law in European Union Member States and for anyone processing data of E.U. data subjects.[39] The Regulation is forward-thinking in that it supports the current technological environment while remaining general enough to protect the privacy rights of individuals throughout future technological advances and data processing uses.[40]

The General Data Protection Regulation was proposed by the European

---

32. Manu J. Sebastian, *The European Union's General Data Protection Regulation: How Will It Affect Non-EU Enterprises?*, 31 SYRACUSE J. SCI. & TECH. L. 216, 223 (2015). *See also How did we get here? An overview of important regulatory events leading up to the GDPR,* EUGDPR.ORG (Oct. 10, 2018), https://eugdpr.org/the-process/how-did-we-get-here/ [https://perma.cc/P8GP-8U6H].

33. *The Principles*, INFORMATION COMMISSIONER'S OFFICE (Oct. 10, 2018), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/principles/ [https://perma.cc/T63Z-MAVW].

34. *Id*. *See also* Commission Regulation 2016/679, 2016 O.J. (L 119) 1 (EU) [hereinafter GDPR].

35. *GDPR FAQs: Frequently Asked Questions about GDPR*, EUGDPR.ORG (Oct. 10, 2018), https://eugdpr.org/the-regulation/gdpr-faqs/ [https://perma.cc/T43N-N85L].

36. Carl Gottlieb, *Introduction To The GDPR*, THE GDPR GUY (Feb. 23, 2017), https://thegdprguy.com/gdpr-introduction/.

37. *How did we get here? An overview of important regulatory events leading up to the GDPR*, *supra* note 31.

38. *Id*.

39. *Id*.

40. *Id*.

Commission on January 25, 2012.[41] The regulation combined concepts from the Data Protection Directive with various laws created by the Member States through their interpretations of the Directive to create a more strict and uniform privacy law for the E.U. and its data subjects.[42] The European Parliament approved an amended version of the regulation on March 12, 2014.[43] After a lengthy proposal, amendment, and approval process, the General Data Protection Regulation was adopted by the Council of the European Union and the European Parliament in April of 2016.[44] The Regulation entered into force in May 24, 2016, and Member States had two years to prepare for full enforcement of the regulation which occurred on May 25, 2018.[45]

The primary purpose of the Regulation is to give data subjects more control over their personal data and to safeguard the right to personal data protection.[46] This Regulation is a positive step toward a more controllable and agreeable data collection, storage and usage system for the data privacy and protection of both adults and children.[47] Additionally, the GDPR has created stricter standards for obtaining consent for data processing than the Data Protection Directive.[48] The GDPR requires clear, informed, affirmative, and "freely given" consent prior to the processing of an E.U. data subject's personal data.[49]

The General Data Protection Regulation helps protect the individual by strengthening the individual's rights to control the usage, retention and movement of their personal data, rather than to simply regulate or apply controls to companies that process data.[50] According to its own Article 1, the GDPR "lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal

---

41. Sebastian, *supra* note 32, at 222.

42. *Id*.

43. *Timeline of Events: An overview of key GDPR events from proposal, amendment, approval, adoption to enforcement*, EU GDPR.ORG (Oct. 10, 2018), https://eugdpr.org/the-process/timeline-of-events/ [https://perma.cc/9MSP-NTMF].

44. *Id*.

45. *The History of the General Data Protection Regulation*, European Data Protection Supervisor (Oct. 10, 2018), https://edps.europa.eu/data-protection/data-protection/legislation/history-general-data-protection-regulation_en [https://perma.cc/QBK6-WD83].

46. Milda Macenaite, *The "Riskification" of European Data Protection Law through a Two-Fold Shift*, 8 EUR. J. RISK. REG. 506, 533 (Sept. 2017).

47. Karen McChullagh, *The general data protection regulation: a partial success for children on social network sites?*, DATA PROTECTION, PRIVACY AND EUROPEAN REGULATION IN THE DIGITAL AGE 110, 131 (2016).

48. Viktor Mayer-Schönberger & Yann Padova, *Regime Change? Enabling Big Data Through Europe's New Data Protection Regulation*, 17 COLUM. SCI. & TECH. L. REV. 315, 325-26 (Apr. 2016).

49. DENIS KELLEHER AND KAREN MURRAY, EU DATA PROTECTION LAW 155 (2018). Under the GDPR, "freely given" consent means that the subject should not feel pressured into giving consent. *Supra* at 156.

50. Gottlieb, *supra* note 36.

data."[51] The Regulation also "protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data."[52] The Regulation further maintains that, "the free movement of personal data within the union shall be neither restricted nor prohibited for reasons connected with the protection of natural persons with regard to the processing of personal data."[53]

As a binding legislative act, the GDPR is to be fully applied across the European Union.[54] The Regulation is enforceable in all Member States and upon any organization that holds or touches information of E.U. data subjects.[55] The Regulation defines "data subjects" E.U. citizens as well as anyone who lives, works or travels through the E.U.[56] The Regulation defines the rights a data subject has over his or her personal information and gives the subject control over how, why, and when his or her personal data is processed.[57]

The Article 29 Working Party ("Working Party") was created by the Data Protection Directive and predated the GDPR as the E.U. advisory authority on data protection matters.[58] After the enactment of the GDPR, however, the European Data Protection Board replaced the Working Party as the independent European body that oversees the application and promotes consistent cooperation and enforcement of data protection rules in the European Union.[59] The Article 29 Working Party continues to publish guidelines for data protection in the E.U. which serve as strong suggestions for implementing the Regulation and have on occasion been enacted into law.

The GDPR applies to all companies or organizations that offer goods or services to, monitor the behavior of, or process or hold the personal data of E.U. data subjects.[60] Companies that process such data, regardless of location, are required to comply with the Regulation.[61] Organizations have strong incentive to

---

51. Regulation (EU) 2016/679, art. 1 § 1.

52. Regulation (EU) 2016/679, art. 1 § 2.

53. Regulation (EU) 2016/679, art. 1 § 3.

54. *GDPR FAQs: Frequently Asked Questions about GDPR, supra* note 35.

55. *How did we get here? An overview of important regulatory events leading up to the GDPR, supra* note 31.

56. Gottlieb, *supra* note 36.

57. P.T.J. Wolters, *The Control by and the Rights of the Data Subject Under the GDPR*, 22 No. 1 J. INTERNET L. 1, at 6.

58. Directive 95/46/EC, of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 1995 O.J. (L 281) 0031-0050, art. 29. *See also* Nadezhda Purtova, *The law of everything. Broad concept of personal data and future of EU data protection law*, 10 LAW, INNOVATION, AND TECHNOLOGY 1, 40-81, 45 (2018), https://www.tandfonline.com/doi/pdf/10.1080/17579961.2018.1452176?needAccess=true [https://perma.cc/Z4TJ-PBQN].

59. GDPR Articles 63-76 and Recitals 135-140. *See also About EDPB*, EUROPEAN DATA PROTECTION BOARD (Jan. 10, 2018), https://edpb.europa.eu/about-edpb/about-edpb_en [https://perma.cc/72RU-UU3R].

60. *GDPR FAQs: Frequently Asked Questions about GDPR, supra* note 35.

61. *Id*.

comply with the GDPR because the costs of non-compliance can be significant.[62] The maximum penalty a regulatory authority can impose for non-compliance is a fine of twenty million Euros or four percent of annual revenue of the parent company.[63] In addition to imposed fines, an organization in non-compliance can be subject to a class action lawsuit for breaches of data subject rights under the Regulation.[64]

The Regulation confers a number of rights upon individuals to enable stronger protections of personal data and privacy in the E.U. These rights include: (1) the right to be informed about how data is processed; (2) the right to access one's personal data; (3) the right to rectification; (4) the right to erasure; (5) the right to restrict processing; (6) the right to ensure third parties are notified of rectification or erasure of personal data; (7) the right to data portability; (8) the right to object generally to the processing of personal data; (9) the right to object specifically to personal data processing for direct marketing purposes; and (10) the right to not be subject to automatic profiling and decision making.[65] Additionally, a data subject always retains the right to object to data processing for direct marketing purposes, regardless of the lawful basis for processing that applies.[66]

The European Union aims to protect the privacy of all E.U. data subjects, and prior to the GDPR the data protection policies grouped adults and minors together without special provisions for the processing of children's data.[67] The GDPR, while strengthening the data protection for all E.U. subjects, has also recognized that children should be specially protected under the regulation.[68] Under the GDPR, children merit special protections ". . . as they may be less aware of the risks, consequences and safeguards concerns and their rights in relation to the processing of personal data."[69] To collect, use, or distribute the personal data of minor data subjects, there are a number of general requirements that must be met under the GDPR.[70]

First and foremost, data processing that is subject to the GDPR will be legal only if it is processed under one of the six legitimate bases laid out in Article 6

---

62. Gottlieb, *supra* note 36.

63. *Id*.

64. *Id*.

65. KELLEHER & MURRAY, *supra* note 49 at 196. *See also Individual Rights*, INFORMATION COMMISSIONER'S OFFICE (Oct. 14, 2018), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/ [https://perma.cc/X6V3-ADAA].

66. *Lawful basis for processing*, INFORMATION COMMISSIONER'S OFFICE (Oct. 10, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/ [https://perma.cc/W5PF-CJ92].

67. Macenaite & Kosta, *supra* note 17, at 148.

68. *Id*.

69. Regulation (EU) 2016/679, Recital 38.

70. *Children*, INFORMATION COMMISSIONER'S OFFICE (Nov. 23), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/applications/children/ [https://perma.cc/49A9-MTTZ].

Part 1 of the GDPR.[71] Having a lawful basis for processing personal data is important because, without a lawful basis, the data processing would breach the first principle of data protection and privacy as a fundamental right.[72] The lawful basis requirement to process personal data is not a new concept.[73] However, different from its predecessors in E.U. data privacy law, the GDPR places a higher emphasis on the accountability and transparency elements of a data processor's lawful basis for processing.[74] The individual's right to be informed under Article 13 and 14 of the GDPR requires that organizations inform data subjects with transparency about the lawful basis for processing their data.[75] This also requires that details regarding the lawful basis for processing data be included in the organization's privacy notice.[76]

Article 6, Part 1 of the General Data Protection Regulation provides six lawful purposes for processing data of a data subject.[77] At least one of the six lawful purposes for processing must apply when personal data is processed, although no basis for processing is more important or compliant than another.[78] The six lawful purposes for processing data of a data subject include: (1) consent, (2) contract, (3) legal obligation, (4) vital interests, (5) public task, (6) legitimate interests.[79]

1. The Lawful Bases for Data Processing Under the GDPR

Data of a data subject may be processed where the individual has clearly consented to the processing of their personal data for a specific purpose.[80] Under the GDPR, consent must be freely given and expressly confirmed, and those consenting should be given ongoing choice and control regarding the processor's use of their data.[81]

Recital 32 of the Regulation requires that consent should be an informed and unambiguous indication of agreement by the data subject to have his or her personal data processed.[82] The agreement should be clear and affirmative, and may be demonstrated by a written or oral statement, or could be demonstrated by

---

71. KELLEHER & MURRAY, *supra* note 49 at 153.

72. *Lawful basis for processing, supra* note 66.

73. *Id*.

74. *Id*.

75. *Id*.

76. *Id*.

77. Regulation (EU) 2016/679, art. 6 § 1.

78. *Lawful basis for processing, supra* note 66.

79. Regulation (EU) 2016/679, art. 6 § 1(a)-(f); *See also Lawful basis for processing*, *Lawful basis for processing, supra* note 66.

80. *Lawful basis for processing, supra* note 66.

81. *Consent*, INFORMATION COMMISSIONER'S OFFICE (Oct. 10, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/consent/ [https://perma.cc/S4K5-H4BX].

82. Regulation (EU) 2016/679, Recital 32.

ticking a box on a website agreement form.[83] The Regulation also states that silence, inactivity, or pre-ticked boxes may not constitute consent, and that the request for consent must be clear, concise, and not overly disruptive to the user in attempting to access a service or website.[84] Further, if a website or service processing data for multiple purposes, the consent agreement should clearly inform the user of each purpose for which the data is processed.[85]

a. Contract

Data may be processed where the processing is necessary for performance of a contract existing between the processor and the data subject, or where the data subject has requested the processor take specific action regarding data collection prior to entering into a contract.[86] This lawful basis may apply to online purchase orders where a controller is required to process the purchasing individual's address to deliver the goods.[87] If a contract has not yet been entered into, this basis may apply if a purchaser requests a quote or assessment from an organization or service provider that requires processing of personal data prior to entering into a contract.[88] An example of data processing that may occur prior to the execution of a formal contract could be an insurance quote provided by an insurer.[89]

b. Legal Obligation

Legal obligations to process data serve as a lawful basis for processing where the processing is necessary for the processor's compliance with the law.[90] For processing to occur under the legal obligation basis, there does not have to be a legal obligation that specifically requires the processing activity.[91] Rather, the processing may be classified under the legal obligation basis if the overall purpose of processing the personal data is to comply with a legal obligation that is sufficiently based in common law or statute.[92] However, this basis cannot be relied upon if the processor has discretion over whether the personal data is

---

83. *Id*.

84. *Id*.

85. *Id*.

86. *Lawful basis for processing, supra* note 66.

87. *Contract*, INFORMATION COMMISSIONER'S OFFICE (Oct. 11, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/contract [https://perma.cc/WS8P-CKE6].

88. *Id.*

89. *Id*.

90. *Lawful basis for processing, supra* note 66.

91. *Legal Obligation*, INFORMATION COMMISSIONER'S OFFICE (Oct. 11, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legal-obligation/. https://perma.cc/9UTN-Z7SZ

92. *Id*.

processed, or if there is another reasonable means of compliance that does not require processing personal data.[93]

c. Vital Interests

Data processing satisfies the lawful basis requirement where processing the data is necessary to protect the life of a data subject.[94] Vital interests as a lawful basis for processing personal data is limited in scope and is intended to apply only to matters of life and death.[95] This lawful basis most likely arises when personal data needs to be processed for medical purposes and the individual is unable to consent to the processing.[96]

The vital interest basis is not appropriate for medical care planned in advance, nor is it the most appropriate basis for larger scale personal data processing.[97] Possible exceptions to the limitations of the vital interest basis could include large-scale processing is in response to a natural or man-made disasters resulting in a humanitarian emergency.[98]

In rare cases, an individual's personal data may be processed to protect the vital interest of another.[99] For instance, it may be necessary to process the personal data of a parent in order to protect the vital interests of a minor child.[100] However, when processing an individual's personal data to protect the vital interests of another, the Regulation indicates that the processor should attempt to process the data under an alternative lawful basis before relying on the vital interest basis.[101]

d. Public Task

Data may be lawfully processed where the processing is necessary for the performance of a public interest task or for an official function, or if the task or function otherwise has a clear basis in law.[102] The public task lawful basis is most relevant to public authorities, although the basis can also apply to an organization that performs tasks in the public interest or exercises official authority.[103] For

---

93. *Id*.

94. *Lawful basis for processing, supra* note 66.

95. *Vital interests*, INFORMATION COMMISSIONER'S OFFICE (Oct. 11, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/vital-interests/ [https://perma.cc/58DY-V9BD].

96. *Id*.

97. *Id*.

98. *Id*.

99. *Id*.

100. *Id*.

101. *Id*.

102. *Lawful basis for processing, supra* note 66.

103. *Public Task*, INFORMATION COMMISSIONER'S OFFICE (Oct. 11, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-

example, a water company, private or public, would likely be able to rely on this basis because the company processes data to carry out public interest functions, specifically the administration of utility services.[104]

To process data under the public task lawful basis, the processing must be necessary.[105] Processing is necessary if it achieves the purpose in the most reasonable, targeted and proportionate way of achieving the means.[106] If there is a less intrusive way of achieving the same result, the processing is likely not necessary. The public task lawful basis is predicated upon the nature of the function being performed by the organization rather than the nature of the organization itself.[107]

e. Legitimate Interests

Data may be lawfully processed where processing is necessary for the processor's or a third party's legitimate interests.[108] However, where there is adequate reason to protect the data subject's personal data, the individual's reasons for data protection will override an organization's legitimate business interests for processing.[109] The legitimate interests lawful basis for processing can be divided into three key components: legitimate interest, necessity of processing, and a balancing test.[110]

For legitimate interests to serve as a lawful basis for processing, it must first be determined whether the processor is pursuing a legitimate interest.[111] Next at issue is whether the data processing is necessary for the processor to achieve that legitimate purpose.[112] Lastly, a balancing test of the individual's interests and the legitimate interests of the processor should be conducted to ensure that the impact of the data processing and risk to the data subject do not greatly outweigh and therefore override the legitimate interests of the processor.[113]

B. Protection of Children's Personal Data under the GDPR

The Data Protection Directive did not contain specific rules regarding data

---

processing/public-task/ [https://perma.cc/45V6-MMZ8].

104. *Id*.

105. *Id*.

106. *Id*.

107. *Id*.

108. *Lawful basis for processing, supra* note 66.

109. *Id.*

110. *Legitimate Interests*, INFORMATION COMMISSIONER'S OFFICE (Oct. 11, 2016), https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/ [https://perma.cc/G8VF-CNKB].

111. *Id*.

112. *Id*.

113. *Id*.

processing of children.[114] In 2011, the European Data Protection Supervisor recognized that children, due to their particular vulnerability, needed stronger protections of their privacy rights.[115] This opinion recognized that the Data Protection Directive did not address the way in which children should be informed about the collection of their data, how the data should be collected, which individuals should be treated as children, or the conditions under which children or their legal representative may exercise their privacy rights.[116]

Further, the Directive did not address the age of consent for children in regard to their data and resulted in various age of consent laws throughout the Member States.[117] The European Data Protection Supervisor suggested that in creating a more protective regulatory framework for children and their privacy rights, an age threshold should be established so that if a child is younger than the threshold, information may only be collected on the child where verifiable and explicit consent has been obtained.[118]

In response to the need for stronger protection of children's information online, the GDPR specifically highlights the fact that children's data merit special protection, and it introduced new requirements for processing of personal information of children.[119]

Article 8, Section 1 provides that where a data processor is relying on consent as a lawful basis for processing, such processing is only lawful where the child is at least sixteen years of age.[120] However, if a child is younger than age sixteen, processing may be lawful "only if and to the extent that consent is given or authorized by the holder of parental responsibility over the child."[121] Despite the regulation setting the age of consent for data processing at sixteen years old, Member States may decide to lower the age of consent for data processing as long

---

114. *A comprehensive approach on personal data protection in the European Union*, EUROPEAN DATA PROTECTION SUPERVISOR ¶ 92, at 19 (Jan. 14, 2011), https://edps.europa.eu/sites/edp/files/publication/11-01-14_personal_data_protection_en.pdf [https://perma.cc/8837-8R3W].

115. *Id*. ¶¶ 92-3, 174.

116. *Id*. ¶ 94.

117. Macenaite & Kosta, *supra* note 17, at 151.

118. *A comprehensive approach on personal data protection in the European Union, supra* note 114, at ¶ 94.

119. GDPR Recital 38. *See also* GDPR art. 8, § 7.1 (EC). *See also What's New?* INFORMATION COMMISSIONER'S OFFICE, (Jan. 4, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/whats-new/ [https://perma.cc/4MJZ-W7CA]. *See also* Article 29 Data Protection Working Party, 17/EN WP259 rev. 01, *Guidelines on Consent under Regulation 2016/679*, 23, § 7.1 (EC).

120. Regulation 2016/679, of the European Parliament and the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), 2016 O.J. (L 119) art. 8, § 1 (EU).

121. *Id*.

as the age is not younger than thirteen years old.[122] The Regulation requires that to obtain informed consent, the information given to the user about the ways in which their data is processed should be understandable to the audience addressed.[123] This means that the controller, if processing children's data, must disclose the intended uses of the collected data in clear and plain language that a child could understand.[124]

Section 2 of Article 8 requires a data controller to "make reasonable efforts to verify . . . that consent is given or authorized by the holder of parental responsibility over the child."[125] What constitutes a "reasonable effort" is a definition in the making; however, the Article states that the "available technology" should be taken into consideration.[126]

The third and final section of Article 8 states that the consent provisions for processing data of children shall not apply to the general contract law the E.U. Member States regarding the validity, formation, or effect of a contract with a child.[127]

Recital 38 of the GDPR provides that the special protections should apply to the processing of children's' data for marketing or data collection purposes or for the purposes of creating personality or user profiles.[128] An exception to the special protections of children's personal data exists: a child does not need the consent of the holder of parental responsibility where preventative or counseling services are being offered directly to a child.[129] This type of exception could arise in a situation where a child tells a teacher or person in a caretaking capacity that the child is being abused. In this type of situation the adult does not need to obtain parental consent in order to report the situation to relevant authorities.[130] Prior parental authorization may also not be required in circumstances where child protection services are offered to a child online through a chat service or similar type of communication for the purposes of protecting the child's wellbeing.[131]

The Article 29 Working Party, in its Guidelines on Consent under Regulation 2016/679, provides that where controllers provide services to children above the age threshold for consent on the basis of consent, the controller is expected to

---

122. *Id*.

123. Article 29 Data Protection Working Party, 17/EN WP 259 rev. 01, *Guidelines on Consent under Regulation 2016/679*, 24, § 7.1 (EC).

124. GDPR Recital 58. *See also* Article 29 Data Protection Working Party, 17/EN WP259 rev. 01, *Guidelines on Consent under Regulation 2016/679*, 24, § 7.1 (EC).

125. Regulation 2016/679, art. 8, § 2 (EC).

126. *Id*.

127. *Id*. § 3.

128. Regulation 2016/679, Recital 38 (EU).

129. *Id*.

130. Luke Irwin, *Navigating GDPR consent for minors,* IT GOVERNANCE EUR. BLOG, (Jan. 26, 2018), https://www.itgovernance.eu/blog/en/navigating-gdpr-consent-for-minors [https://perma.cc/T96E-NYEH].

131. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259, § 7.1.4 at 27 (EC).

make reasonable efforts to verify that the user is in fact above the age of digital consent.[132] These measures should be proportionate to the nature of the data processing and the risks associated with processing the information collected.[133] The controller should take care to ensure that users who state they are above the age of digital consent are indeed above the age of digital consent.[134] Although the GDPR does not explicitly require such verification, if a controller processes data without valid consent as defined in the regulation, the data processing will be unlawful.[135]

However, where a child indicates that he or she is younger than the age of digital consent, the controller may accept this age statement without further verification of the child's age but must then obtain verifiable parental consent to process the child's data.[136] Upon receiving parental authorization, the controller should take steps to ensure that the person providing the consent to process the child's data has appropriate parental authority.[137]

The Regulation does not offer practical methods or solutions for obtaining verifiable and reliable parental consent for the processing of a child's data.[138] The Working Party suggests controllers take a proportionate approach to ensuring that the user providing consent for processing the child's data has appropriate parental authority to do so.[139] Under this approach, processing that is considered "low-risk" to the child may require less information for confirming the parent's identity, like an email, whereas "high-risk" processing may require more information from the parent. [140] For example, a controller may ask a parent to make a nominal payment via a bank transaction that contains a confirmation in the transcription's description that the holder of the bank account has parental authority over the child seeking information society services.[141]

III. HISTORY OF DATA PRIVACY AND CURRENT CHILD PRIVACY LAWS IN THE U.S.

A. History of Data Privacy in the U.S.

In the United States, the right to privacy has been recognized in the legal realm since the late 1800s when Samuel D. Warren and Louis Brandeis published

---

132. *Id*. § 7.1.3 at 25.

133. *Id*.

134. *Id*.

135. *Id*.

136. *Id*.

137. *Id*.

138. *Id*. § 7.1.4 at 26.

139. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259, § 7.1.4 at 26 (EC).

140. *Id*.

141. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679,* 17/EN WP259, n. 66 at 26 (EC).

"The Right to Privacy" in the Harvard Law Review. In 1890, Warren and Brandeis recognized that the development of a right to privacy was inevitable, as "solitude and privacy have become more essential to the individual; but modern enterprise and invention have, through invasions on his privacy, subjected him to mental pain and distress . . . ."[142] The authors observed that, "[r]ecent inventions and business models call attention to the next step which must be taken for the protection of the person, and for securing to the individual . . . the right "to be let alone."[143] This precise premise continues to drive the development of privacy laws and data protection regulations today.

Privacy rights first started appearing in the common law of torts, where criminal and civil remedies existed for the use of a person's picture or personal identity without consent for advertisement.[144] Privacy rights, although not expressly enumerated as a right in the Constitution, have been upheld by the Supreme Court as a constitutionally protected right in a number of cases.[145] In 1965, the Supreme Court first recognized the constitutional right to privacy in the *Griswold v. State of Connecticut* ruling that the right to privacy within a marital relationship is a fundamental right that the State cannot constitutionally abridge.[146]

As technology has advanced and computer usage has increased, Americans have become more concerned about their records held by the Government because of the Government's ability and power to investigate and store information.[147] In response to this ever-growing concern, Congress enacted the Privacy Act of 1974 (5 U.S.C. 552a).[148]

The Privacy Act of 1974 aims to minimize the Government's informational privacy intrusions on citizens while balancing the government's legitimate interests to function efficiently.[149] The Privacy Act of 1974 prevents the federal government from disclosing, collecting, or using personal information without proper authorization from the person about whom the data is collected.[150]

Because the Privacy Act of 1974 applies only to the federal government, a patchwork of data and information privacy laws emerged to protect more specific types of information and groups of people.[151] Several laws following The Privacy

---

142. Samuel D. Warren, Louis D Brandeis, *The Right to Privacy*, 4 HARV. L. REV. 193, 196 (1890).

143. *Id.* at 195.

144. Haeji Hong, Esq., *Dismantling the Private Enforcement of the Privacy Act of 1974: Doe v. Chao* (2005), 38 AKRON L. REV. 71, at 74-79.

145. *Id.* at 76.

146. *Griswold v. Connecticut*, 85 S.Ct. 1678, 1690 (1965). *See also* Hong, *supra* note 144, at 83.

147. S. Rep. No. 93-1183 (1974).

148. Hong, *supra* note 144, at 83.

149. *Id.*

150. *Id.*

151. *Id.* at 84. *See also* Holly Kathleen Hall, *Oversharenting: Is it really your story to tell?*, 33 J. MARSHALL J. INFO. TECH. & PRIVACY L. 121, 132 (2018).

Act of 1974 include the Health Insurance Portability and Accountability Act ("HIPPA"), the Fair Credit Reporting Act ("FCRA"), the Driver's Privacy Protection Act ("DPPA") and the Children's Online Privacy and Protection Act ("COPPA" or "the Act").[152]

1. Protection of Children's Personal Data Under COPPA

In the United States prior to 1998, no federal restrictions or regulations for children's data or children's online privacy existed.[153] As the use of the Internet, especially by children, increased, so did the concerns of parents and the government regarding children's information being shared with third parties.[154] Congress found that protecting the privacy of children's personal information online was a compelling government interest, to which instating defenses for the protection of children's Internet privacy is the least restrictive means.[155] In efforts to protect the privacy of children, Congress enacted the Children's Online Privacy Protection Act (15 U.S.C. §§ 6501-6508) to regulate the collection, use, and disclosure of personal data of minors under the age of thirteen.[156] The Act became effective in April of 2000 and was revised in 2013 by the Federal Trade Commission to reflect the rapid pace of change in technology and the online environment.[157]

Congress applies the COPPA protections to children under thirteen years of age, recognizing that children younger than thirteen years old may not fully understand the safety and privacy concerns regarding online collection of personal information, which also makes them more susceptible to overly invasive or overreaching marketing techniques.[158] Policymakers in the U.S. deemed children under age thirteen too young to provide consent online and drew a

---

152. Hall, *supra* note 151.

153. Alexis M. Peddy, *Dangerous Classroom "App"-Titude: Protecting Student Privacy From Third-Party Educational Service Providers*, B.Y.U. EDUC. & L.J. 125, 132 (2017).

154. *Id*.

155. *Id*.

156. *Id*. at 133.

157. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2013), https://www.ftc.gov/system/files/2012-31341.pdf [https://perma.cc/K6X2-VXR6]. *See also Children's Online Privacy Protection Rule: Not Just for Kids' Sites,* FEDERAL TRADE COMMISSION: PROTECTING AMERICA'S CONSUMERS (April 2013), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-not-just-kids-sites [https://perma.cc/4C2Z-Y387] and *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business,* FEDERAL TRADE COMMISSION: PROTECTING AMERICA'S CONSUMERS (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/3UNR-4B79].

158. *Complying with COPPA: Frequently Asked Questions*, FEDERAL TRADE COMMISSION – PROTECTING AMERICA'S CONSUMERS (March 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions [https://perma.cc/WEY4-MBU7].

seemingly arbitrary line between children above and below the age of thirteen.[159] While there is no remarkable difference between the ability of twelve and thirteen year-olds to safely navigate the Internet, teenhood seems to be a fairly standard subjective line for regulatory benchmarks.[160] In addition to online consent, thirteen years serves as a benchmark for movie ratings (PG-13 movies) and is the age at which a child can begin working part-time in the United Kingdom.[161]

The Act defines "child" as an "individual under the age of thirteen," and for the purposes of this note, "child" or "minor" will be construed as the same.[162] For the purposes of data protection for children under COPPA, the Act casts a broad net over what constitutes "personal information."[163] "Personal information" includes categories of information that can be used to identify and contact a specific person.[164] This information may include a child's name, address, online contact information or screenname, telephone number, or social security number.[165]

"Personal information" was expanded in 2013 to include "persistent identifiers," which include information that can be connected to a user over time and across web sites or services.[166] Persistent identifiers may include a customer number contained within a cookie, an Internet Protocol (IP) address, a device serial number, a photograph or audio file containing a child's information, or geolocation information precise enough to connect the user with a street and city or town.[167] Personal identifiers may also include other information about the child or the child's parents that is collected and combines with other identifiable information in order to track a user across online forums.[168]

The Act defines "collecting" as gathering information, or prompting or encouraging a child to share information that the operator may then store or use.[169] "Collection" is defined in this way to ensure the understanding that an

---

159. Rachel Withers, *13 Going on Old Enough to Share Your Personal Data*, SLATE (Apr. 24, 2018), https://slate.com/technology/2018/04/why-not-apply-the-childrens-online-privacy-protection-act-to-everyone.html. [https://perma.cc/2EDL-68KD].

160. *Id*.

161. *Id*. *See also* Child Employment, GOV.UK (Jan. 20, 2019), https://www.gov.uk/child-employment [https://perma.cc/DW67-EKZU].

162. 16 C.F.R. § 312.2 (2013).

163. Reyes et al., *"Won't Somebody Think of the Children?" Examining COPPA Compliance at Scale,* 2018 PROCEEDINGS ON PRIVACY ENHANCING TECHNOLOGIES 63, 65 (2018).

164. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013).

165. *Complying with COPPA: Frequently Asked Questions*, FEDERAL TRADE COMMISSION – PROTECTING AMERICA'S CONSUMERS (Mar. 2015), https://www.ftc.gov/tips-advice/business-center/guidance/complying-coppa-frequently-asked-questions [https://perma.cc/2CV9-WVKL].

166. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013).

167. *United States of America v. LAI Systems, LLC*, Case No. 2:15-cv-9691 at 6, (2016). *See also* 16 C.F.R. § 312.5(d), 3982.

168. *United States of America v. LAI Systems, LLC*, Case No. 2:15-cv-9691 at 6, (2016). *See also* 16 C.F.R. § 312.1.

169. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2(A)(1)(a) (2013).

operator will be responsible for data it collects on a child where an open forum for the child to enter information was provided, regardless of whether the information is required for the child to participate in the activity, or whether the information is intentionally gathered.[170] Operators should have a COPPA-compliant plan in place for providing notice to parents and obtaining consent from parents the moment the child's data is gathered.[171] If there is no such plan in place, it will be too late to obtain parental consent once the child has posted or provided personal information online.[172]

The Children's Online Privacy Protection Act provides guidelines regarding the collection of personal data about minors.[173] The Act applies to owners and operators of Internet sites or online services that collect children's personal data and are partially or wholly directed toward children.[174] Typically, sites that must be COPPA compliant fall under one of the following categories: (1) sites directed toward children, (2) sites directed toward general audiences where the operators have actual knowledge that the site collects data from children, or (3) where the operators have actual knowledge that the site collects information directly from users of another site or service that is directed toward children.[175] The Act requires compliance from websites or services that are directed toward children or directed toward a general audience if it also collects children's personal information as part of the general audience.[176] Ultimately, if the website or online service is targeted toward children or has actual knowledge that it collects personal information from children, the website or online service should comply with COPPA.[177]

These online privacy protections for children are monitored and enforced by the Federal Trade Commission ("FTC").[178] The Act does include a "safe harbor" provision which allows industry groups, if approved by the FTC, to create and implement the Rule's protections in a self-regulatory manner.[179] It requires that services or websites collecting data of children obtain verifiable parental consent prior to the collection of such data.[180] Obtaining "verifiable consent" means making a reasonable effort to ensure that, prior to collecting information about a child, a parent of the child receives notice of the website or service's collection, use, and disclosure practices of personal information, and that the parent

---

170. *Id*.

171. *Id*.

172. *Id*.

173. *Internet* Privacy, Executive Legal Summary 387, WESTLAW (2018).

174. *Id*.

175. Reyes et al., *supra* note 163, at 64.

176. *Internet Privacy*, *supra* note 173.

177. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013). *See also* Macenaite & Kosta, *supra* note 17, at 174.

178. *Internet* Privacy, Executive Legal Summary 387, WESTLAW (2018).

179. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2013).

180. Macenaite & Kosta, *supra* note 17, at 168.

authorizes the use of the personal information.[181]

Further, the Act restricts operators of websites or web services from conditioning a child's participation in online activities on the collection of personal information beyond what is reasonably required to participate in the online application.[182]

Much like the GDPR's requirements for consent, the COPPA requires entities to provide parents or legal guardians with the tools to make informed decisions about their children's data and the power to control how their children's personal data is collected and used.[183] The Act gives parents or legal guardians more control over their child's data by requiring that entities provide clear and understandable disclosure of personal data collection practices, as well as how and with whom collected data is shared.[184] The Act further requires the entity to obtain verifiable parental consent before collecting, using, or sharing personal data of children.[185]

As for obtaining verifiable consent, the Act does not offer universal methods for gathering such consent, but rather that the operator must make "reasonable efforts to obtain verifiable parental consent, taking into account available technology."[186] Generally, COPPA requires that an operator obtain verifiable parental consent prior to gathering personal information from a child younger than thirteen years old.[187] However, several exceptions to the strict consent rules of the Act do exist.[188] In such exceptional circumstances, the type of information that can be collected under each exception is limited and the information may not be disclosed for any reason other than the specific purposes for which it was collected.[189]

For example, an operator may collect the name or online contact information of the parent or child for the purposes of providing notice to the parent about data protection policies and to obtain verifiable consent as required by the Act; however, if the operator has not obtained such consent within a reasonable time after the collection of the initial data, the information must be deleted from all records.[190] The Act also provides exceptions when the sole purpose of collecting

---

181. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.2 (2013).

182. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2013).

183. Reyes et al., *supra* note 163, at 64.

184. *Id.* at 65.

185. *Id*.

186. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2013). *See also* Reyes et al., *supra* note 163, at 64, 65.

187. *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business,* FEDERAL TRADE COMMISSION: PROTECTING AMERICA'S CONSUMERS (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/3UNR-4B79].

188. *Id*.

189. *Id*.

190. *Complying with COPPA: Frequently Asked Questions*, FEDERAL TRADE COMMISSION – PROTECTING AMERICA'S CONSUMERS (March 2015), https://www.ftc.gov/tips-advice/business-

online contact information of a minor is for the purposes of responding directly to a child's one-time request.[191] This exception requires that the child's contact information not be used to contact the child for any other purpose or on any other occasion except to respond to the request at issue.[192] After submitting the one-time response to the child's request, the child's contact information must be promptly deleted from all records.[193]

An operator's collection of a child's contact information may also fall into several other exceptions which focus on the safety of the child, precaution against liability, or compliance with other law enforcement, judicial process, or public safety needs or concerns.[194] This information, if collected without proper consent, shall not be used to contact the child, including through methods of behavioral advertising, and shall not be used to build a data profile on the child, or for any other purpose.[195]

An operator may also collect information only in the form of a persistent identifier for the purposes of providing support for internal operations of the site or service.[196] The COPPA does not allow any personal information collected from children to be used for profiling, behavioral advertising, or cross-device tracking.[197]

IV. ANALYSIS OF CURRENT ISSUES AND POTENTIAL IMPROVEMENTS TO CHILD PRIVACY REGULATIONS IN THE E.U.

The GDPR is the European Union's first regulation to recognize children as a group requiring special data protection measures, and in providing such special protection, has introduced numerous changes from past data protection laws.[198] As discussed, one of these major changes takes effect where the processing of a child's data is based on the lawful basis of consent, and this change faces a number of practical challenges due to its recent enactment, lack of clarity and absence of uniformity for the Member States.[199]

A. Consent as the Lawful Basis for Processing Children's Data

Consent, although it maintains its own challenges for effective

---

center/guidance/complying-coppa-frequently-asked-questions [https://perma.cc/2CV9-WVKL].

191. *Id*.

192. *Id*.

193. *Id*.

194. *Id*.

195. *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, FEDERAL TRADE COMMISSION: PROTECTING AMERICA'S CONSUMERS (June 2017), https://www.ftc.gov/tips-advice/business-center/guidance/childrens-online-privacy-protection-rule-six-step-compliance [https://perma.cc/ZTX5-UBPP].

196. *Id*.

197. Reyes et al., *supra* note 163, at 65.

198. Macenaite & Kosta, *supra* note 17, at 148.

199. Macenaite & Kosta, *supra* note 17, at 151.

implementation, is the most popular and straightforward method for legitimizing online data processing.[200] Consent is popular for processing the data of children as well because it places the decisions regarding the child's data in the hands of their parents or guardians.[201] While some adults may be ignorant of the privacy risks posed to their child and may agree to any type of processing without fully understanding the ramifications, the GDPR empowers parents to give or withhold consent and to make decisions regarding when, how, and why their child's data is processed.[202] This primary purpose of the GDPR, which gives individuals more control over their personal data and to establish stronger rights to individuals' privacy, also extends to children.[203]

Other options like effective age-blocking or a complete prohibition of processing the data of children under age thirteen provide their own challenges.[204] These options are difficult to effectively achieve, and a full prohibition on collecting children's data disincentivizes web developers and companies from creating new content because data collection is the primary form of monetization online.[205]

The consent requirements under the GDPR apply to all individuals which includes children, but the Regulation does not contain consent provisions specific to children.[206] The GDPR takes an important step forward in creating stricter standards for what constitutes informed consent, although it does not adequately address consent and privacy protection in regard to children.[207] Obtaining consent from a child who does not fully understand the information provided by a data processor or understand the ways in which their data is going to be processed cannot truly equate to meaningful, informed consent.[208]

In most circumstances, a child is not deemed able to provide informed

---

200. Lina Jasmontaite & Paul De Hert, *The EU, Children Under 13 Years and Parental Consent: A Human Rights Analysis of A New, Age-Based Bright-Line for the Protection of Children on the Internet*, INTERNATIONAL DATA PRIVACY LAW 2, 3 (2014).

201. Karen McCullagh, *The General Data Protection Regulation: A Partial Success For Children on Websites?* DATA PRIVACY AND EUROPEAN REGULATION IN THE DIGITAL AGE 110, 127 (Tobias Brautigam & Samuli Miettinen eds., 2016).

202. *Id.*

203. Regulation 2016/679, of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC ("GDPR"), 2016 O.J. (L 119) para.38 (EU). *See also* GDPR art 8 §1. *See also: What's New?* INFORMATION COMMISSIONER'S OFFICE, (Jan. 4, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/whats-new/ [https://perma.cc/FTN3-CXF2].

204. Macenaite & Kosta, *supra* note 17, at 169.

205. Interview with Meaghan Zore, Professor of Law, Indiana University Robert H. McKinney School of Law, in Indianapolis, Ind. (Jan. 23, 2019).

206. Jasmontaite & De Hert, *supra* note 200, at 3.

207. *Id*.

208. *Id*.

consent for their own data processing.[209] Most online services directed toward children would not require processing under the lawful basis of contract, legal obligation, public task, or vital interests; however, while the processing usually falls under consent, some processors may attempt to process children's data under the basis of legitimate interest.[210]

Although legitimate interest is a viable basis under which a child's data could be processed, consent remains the strongest method of currently available under the regulation for protecting children's online data. Consent is the most protective lawful basis for processing children's data because almost any type web service, whether an online application, store, chatroom, game provider, or educational tool, could argue legitimate interests and therefore not be required to obtain consent from a legal guardian prior to collecting and using a child's data.

If a web service relies on legitimate interests as a lawful basis for processing a child's data, the web service could claim, without substantial support, that they have a real business reason for collecting data on children that outweighs the privacy rights of the child. In doing so, a web service could claim that their legitimate business interest of gathering data for the purposes of targeted advertising toward a child outweighs the child's rights to privacy. The GDPR does not specifically prohibit controllers from utilizing automated decision-making practices, like profiling or behavioral advertising, in regard to children and their personal information.[211]

Using legitimate interests rather than consent as a means for lawfully processing children's data would not necessarily ensure children are more protected. If parents want control over how their child's data is used, or if the regulation aims to give parents control to protect their children's rights, children's data should only be processed with parental consent. If a controller processes personal data under the legitimate interest basis, the data subject has the right to object to the processing, although the objection does not necessarily mean the controller must cease the processing.[212] Rather, if a data subject objects to the controller's processing under legitimate interests, the controller may have an opportunity to defend its decisions to process the data.[213] Where the controller has sufficiently shown that the legitimate interest in processing the data outweighs the potential risks of harm to the data subject, the controller may continue to process the data despite the subject's objections.[214]

In contrast, however, if a controller relies on consent to process data, the data subject has the right to withdraw consent at any time and the data processing must

---

209. *Id*.

210. Jasmontaite & De Hert, *supra* note 200, at 2.

211. Article 29 Data Protection Working Party, *Guidelines on Automated individual decision-making and Profiling for the purposes of Regulation 2016/679*, 17/EN WP 251, 26 (EC).

212. International Association of Privacy Professionals [IAPP], *Guidance on the use of Legitimate Interests under the EU General Data Protection Regulation*, DATA PROTECTION NETWORK, Oct. 7, 2017, at 8. *See also* Regulation 2016/679, art. 21 (EU).

213. *Id*.

214. *Id*.

cease immediately.[215] Otherwise, without collecting parental consent, the parent may not know the child is accessing a site or that the site is collecting data and will therefore not be able to control or protect their child's data and privacy rights online. Processing a child's data under legitimate interests and without obtaining parental consent would counteract the overall purpose of the GDPR, which is to provide individuals with more control over their privacy rights, especially in the online world.

Research has shown that developmental stages impact how youth make decisions and that youth under the age of thirteen may not understand the implications of consenting to the disclosure of their personal information online.[216] The typical child does not have the same decision-making abilities as adults, and youthful discretions, like whether to allow an online application or service to post a video the child has taken or sell the child's name and address to third-party providers, should not necessarily follow them into adulthood.[217] Rather than relying on the lawful basis of legitimate interests when collecting data on children, processors should rely solely on processing under consent, because processors will then be required to obtain parental consent if they intend to collect data about a child. This would afford parents the most control over the way their child's data is processed. The GDPR could eliminate the possibility of companies processing data under the legitimate interest basis or another basis that does not adequately protect children or provide parents with control over how their child's data is used by including a provision that allows for the processing of children's data only under the lawful basis of consent.

In the United States, COPPA prohibits online services or websites from collecting the data of children under age thirteen without first obtaining verifiable parental consent.[218] In addition to obtaining consent, a website or online service must provide complete disclosure to the parents of a child regarding the information the service intends to collect and the way in which it will be used, and the service must also ensure that the disclosure has been provided directly to parents.[219] Otherwise, without meeting these requirements, the online tracking of children is non-compliant with COPPA and therefore illegal.[220] Further, COPPA clearly states that operators may not gather information on children for the purposes of behaviorally targeted advertising without parental consent.[221]

Conversely, under the GDPR, there are circumstances in which a child's

---

215. *Id*.

216. Ilaria Liccardi et al., *Can apps play by the COPPA Rules?*, 2014 TWELFTH ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, 2, 3 (2014).

217. Interview with Meaghan Zore, Professor of Law, Indiana University Robert H. McKinney School of Law in Indianapolis, Ind., (Jan. 23, 2019).

218. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2013).

219. *Children's Online Privacy Protection Rule: A Six-Step Compliance Plan for Your Business*, *supra* note 195.

220. Children's Online Privacy Protection Rule, 16 C.F.R. § 312.5 (2013).

221. *Id*.

personal data may be used for targeted marketing.[222] Some services may be permitted to send marketing messages to children based on their personal data or may display targeted advertisements to the children online as long as the service has a lawful basis for doing so.[223] While web services engaging in these direct marketing techniques are strongly encouraged to ensure children's data is specifically protected and that children are fairly informed about the ways in which their data could be used, the GDPR could better protect children if the governing bodies enforce stricter compliance with the Regulation.

The U.S. COPPA is clear that children's data cannot be collected or used without clear consent from a parent, and the GDPR certainly leaves when, how, and under what lawful basis children's data may be used much more open to the web service provider's interpretation or choice.[224] The Regulation would provide better protection for children online by implementing more direct, clear standards for how and for what purposes a child's data may be collected and used.

B. Uniform Age of Consent

It is seemingly contradictory, that while a major goal of the GDPR was to create a uniform data protection framework for data processors and data subjects throughout the European Union, the age at which a child is permitted to consent to the processing of their own data managed to be left for the Member States to decide.[225] Article 8 of the GDPR set the default age of consent for children to agree to the processing of their data to sixteen years old but allows each Member State to set their own age restrictions on consent so long as the age is not younger than thirteen years old.[226] As demonstrated in the figure below, Article 8 leaves the issue of age of consent at essentially the same place it was prior to the implementation of the GDPR: without a uniform age of consent at which children can agree to their data processing by themselves.[227]

---

222. *What if we want to target children with marketing?* INFORMATION COMMISSIONER'S OFFICE, (Jan. 19, 2019), https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/children-and-the-gdpr/what-if-we-want-to-target-children-with-marketing/ [https://perma.cc/R9M6-YDT6].

223. *Id*.

224. van der Hof, *supra* note 1, at 422-23. *See also* Macenaite & Kosta, *supra* note 17, at 171.

225. Macenaite & Kosta, *supra* note 17, at 152.

226. *Id*. at 148.

227. Macenaite & Kosta, *supra* note 17, at 179.

Figure 1.[228]

Despite the GDPR's aims to harmonize data privacy laws across Europe and provide those who process data a simple framework to adhere to, the lack of a uniform age of consent affects children and businesses.[229] The lack of conformity of age of consent also creates significant challenges for cross-border companies or those who provide international services across the E.U.[230] As evidenced in the Figure above, the digital marketplace in the European Union remains without consistent provisions regarding the age upon which consent relied upon as the lawful basis for collecting and using data of an individual.[231]

Further, children are treated as adults under the GDPR once they are older than the required age of consent for that particular country.[232] This means that

---

228. Claire Quinn, *GDPRkids: Age of "Digital" Consent*, PRIVO (2018), https://www.privo.com/blog/gdpr-age-of-digital-consent [https://perma.cc/AZP7-SHDY].

229. Michael Monajemi, *Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information*, 25 U. MIAMI INT'L & COMP. L. REV. 371, 379 (2018). *See also* Sonia Livingstone, *Children: A Special Case for Privacy?* 46 INTERMEDIA 18, 21 (2018), http://www.iicom.org/images/iic/intermedia/july-2018/im-july2018-childrenspecialcaseforprivacy.pdf [https://perma.cc/HEE8-PARP].

230. Sonia Livingstone, *Children: A Special Case for Privacy?, supra* note 229.

231. Macenaite & Kosta, *supra* note 17, at 167.

232. *What does the European General Data Protection Regulation mean for children in the UK?*, LSE: MEDIA POLICY PROJECT 4 (Jan. 7, 2019), http://blogs.lse.ac.uk/mediapolicyproject/files/2018/05/GDPRroundtableLSEfinal.pdf [https://perma.cc/2GZG-MDUK].

under the GDPR, if a country considers a minor to be a child under the age of thirteen, a thirteen year old child will receive the same protections as an adult without additional protections or separate, more age-appropriate descriptions of how their data will be collected or used.[233]

The Working Party has encouraged the Member States to work toward a harmonized solution regarding the lack of age of consent conformity amongst the Member States.[234] If the Member States convened and settled upon a uniform age of consent throughout the E.U., it would help eliminate some currently existing unnecessary challenges experienced by those implementing and enforcing children's online privacy rights under the GDPR.[235]

In the Article 29 Working Party's Guidelines on Consent for the GDPR, it states that a controller must take into account the groups targeted by its services and must be aware of the different national laws regarding age of consent.[236] Further, the Working Party advises that controllers providing cross-border services may need to comply with the laws of each Member State within which it offers services, in addition to complying with the Member State in which it is established.[237]

C. Clarification of Terms and Methods

The GDPR, as currently implemented, is ineffective in part because it lacks definitive provisions for major components of its child protection regulations. The Regulation would be more effectively enforceable with the clarification of terms and requirements, including "directed toward children," "reasonable efforts," and "verifiable parental consent." As the regulation currently defines them, and without much in the way of precedent or past regulatory decisions regarding these matters, practical challenges arise to these idealistically straightforward protection terms and measures.[238] The challenges are manifesting as companies attempt to implement GDPR-compliant policies and as parents attempt to cash in on their GDPR-given rights to having more control over the way their child's data is processed.[239]

1. "Directed Toward Children"

A major difficulty in the enforcement of the GDPR for children's privacy is determining exactly what services and applications ("apps") fall under the

---

233. *Id*.

234. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 24, § 7.1.3 (EC).

235. van der Hof, *supra* note 1, at 424.

236. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 24, § 7.1.3 (EC).

237. *Id*.

238. Macenaite & Kosta, *supra* note 17, at 148, 170.

239. *Id*.

"directed toward children" category.[240] Online service providers, the data subjects, and the enforcement agencies would undoubtedly benefit from a clearer understanding of what constitutes a web service that is "directed toward children."[241]

The GDPR could also better protect children by implementing a system for screening online service users to ensure that data is not collected about children inappropriately or without the knowledge of either the child, the parent or guardian of the child, or the service provider. In recent years, machine learning classifiers have been developed to identify apps designed for children by evaluating text-based and image-based features within the app.[242] These classifiers can determine whether an app belongs to a common category for kids apps, like "education," "games," "comics" or "entertainment" and takes into account the content rating as identified by the app distributor.[243] The classifier may also focus on the title and readability of the app's description, as well as bright colors that may be associated more heavily with children-directed apps.[244]

These types of classifiers could serve three key function in supporting the children privacy and protection effort.[245] First, the classifiers could help regulators like the FTC and the data protection supervisors in the European Union by helping the regulators identity potentially problematic apps.[246] Second, the classifiers could help parents decide whether to download an app for their child by identifying potential privacy issues that may exist within the app or its services.[247] Third, the classifiers could support the app distributors by flagging apps whose privacy practices may require further inspection or by identifying potential legal issues with the app's privacy practices and informing the responsible party.[248]

This type of technology should be used for determining whether applications and web services are "child directed" and whether the apps and services have taken appropriate actions to ensure they are lawfully processing the data of children in accordance with the GDPR. These classifiers could be used by the data protection agencies to help ensure that sites and services that should comply do comply with the child protection laws under the GDPR.

Further, app stores could benefit from the same technology and play a more responsible role in determining whether or not the apps they distribute are "directed toward children." Unfortunately, the recent prevalence of data breaches

---

240. *Id*. at 170.

241. *Id*.

242. Minxing Liu, Haoyu Wang, Yao Guo, Jason Hong, *Identifying and Analyzing the Privacy of Apps for Kids*, Proceedings of the 17th International Workshop on Mobile Computing Systems and Applications, 106 (February 23- 24, 2016).

243. *Id*. at 107.

244. *Id*.

245. *Id*. at 106.

246. *Id*.

247. *Id*.

248. Liu, Wang, Guo, & Hong, *supra* note 242.

and growing uproar about invasive informational gathering tatics reinforces that websites and services providers cannot always be held accountable for self-identifying whether or not they are directed toward certain audiences or compliant with the relevant regulations.[249]

A major aspect of the GDPR is its flow-down design that requires services to certify that the sub-processors that processors interact with are also GDPR-compliant.[250] The enforcement of child protections under the GDPR could be stronger if app stores shouldered more responsibility for monitoring the apps offered and distributed. The app stores could implement a system, like the classifiers and other intelligence technology, to determine which of the apps it distributes and profits from are "directed toward children" and are therefore required to be compliant with the GPDR provisions related to children. The Apple App Store has trended in this direction with its paternalistic approach to its app review process and the precautions it takes when publishing apps that are targeted toward younger populations. Apple's "App Review Guidelines" make clear that Apple will "reject apps for any content or behavior that [it] believes is over the line," and that if an app developer attempts to "cheat the system (for example, by trying to trick the review process, steal user data . . .)" the apps will be removed from the store and the developer will no longer be able to participate in the App Store program.[251]

2. "Reasonable Efforts"

Article 8.2 requires that the controller make reasonable efforts to verify that the consent given is from the holder of parental authority over the child, although it is unclear how much effort and proof needs to be shown by the controller to sufficiently demonstrate compliance with this requirement.[252] The Regulation provides that "reasonable" efforts should be considered along with available technology, and the Working Party suggests to consider whether a child has an "identity footprint" at the time consent is gathered or whether parental

---

249. *See generally In re* Facebook, Inc., 2019 U.S. Dist. LEXIS 14256. *See also* Complaint, Balderas v. Tiny Lab Productions, et al., US District Court of New Mexico. *See also* Shelia A. Millar & Tracy P. Marshall, *New Enforcement Actions For COPPA's 20th Anniversary*, LAW 360: A LEXIS COMPANY (Jan. 2019), https://www.law360.com/articles/1114765/new-enforcement-actions-for-coppa-s-20th-anniversary [https://perma.cc/R63E-997S].

250. Regulation (EU) 2016/679, art. 28. *See also* Regulation (EU) 2016/679, Recital 81.

251. App Review Guidelines: The Comic Book, APPLE INC. (2016), https://devimages-cdn.apple.com/app-store/review/guidelines/App-Review-Guidelines-The-Comic-Book.pdf [https://perma.cc/A469-464L]. The "App Review Guidelines" further address what it considers to be over the line. "What line, you ask? Well, as a Supreme Court Justice once said, 'I'll know it when I see it'. And we think you will also know it when you cross it."

252. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 24, § 7.1.3 (Nov. 28, 2017). *See also* Macenaite & Kosta, *supra* note 17, at 195.

responsibility is difficult to check.[253] While controllers are expected to continually review their processes for verifying consent and the technology available to do so, this portion of the Regulation does not define "reasonable efforts" for obtaining consent to the extent that COPPA does.[254] For the purposes of consent, COPPA provides a usable guide from which the GDPR can continue working toward its comprehensive approach to data protection and privacy.[255]

3. "Verifiable Parental Consent"

While the Regulation provides some guidance for what may constitute proper consent to process children's data, the rules for "verifiable parental consent" need significant clarification.[256] As currently enforced, the GDPR does not offer practical methods or solutions for gathering verifiable parental consent to process a child's data.[257]

D. Consistent Enforcement Methods

The lack of clear expectations and compliance tools when it comes to protecting children's online data causes challenges to the new data protection regulation in the E.U.[258] Enforcement is a difficult task for any type of regulation or legal system, and the GDPR and COPPA face similar challenges in this regard.[259] The current lack of a systematic of enforcement makes it difficult for data protection authorities to ensure controllers are properly protecting the privacy rights of children.[260]

The enforcement of data protection for children under the GDPR could be more effective if the regulation prohibits web services from operating under a "mixed audience" concept. This would mean that rather than providing a web service that lumps all users into one group and treats adults and children similarly in regard to their data, adults and children will have to be differentiated and

---

253. GDPR art. 8 § 2. *See also* Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 26, § 7.1.4 (Nov. 28, 2017).

254. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 26, § 7.1.4 (Nov. 28, 2017). *See also* Foley Hoag LLP, *Cybersecurity 2019 – The Year in Preview: COPPA, the GDPR, and Protecting Children's Data*, JD SUPRA (Dec. 20, 2018), https://www.jdsupra.com/legalnews/cybersecurity-2019-the-year-in-preview-49904/ [https://perma.cc/R36U-M2PP].

255. *See* Foley Hoag LLP, *Cybersecurity 2019 – The Year in Preview: COPPA, the GDPR, and Protecting Children's Data*, JD SUPRA (Dec. 20, 2018), https://www.jdsupra.com/legalnews/cybersecurity-2019-the-year-in-preview- 49904/ [https://perma.cc/R36U-M2PP].

256. Macenaite & Kosta, *supra* note 17, at 186.

257. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 26, § 7.1.4 (Nov. 28, 2017).

258. Macenaite & Kosta, *supra* note 17, at 195.

259. *Id.* at 191.

260. *Id.* at 194.

treated appropriately for their age. Specifically, services would be required to distinguish the users under the age of thirteen, provide age-appropriate privacy policies, and obtain verifiable parental consent prior to the child's use of the web services or the service's collection of any data about the child.

Additionally, prohibiting the "mixed audience" concept would hold data processors more accountable for their processing, especially if it includes processing the data of minors and the "actual knowledge" test.[261] If processors are required to be more purposeful about whether their services target children, processors would have a more difficult time claiming they were "unaware" that children were using the site and its services. This would encourage the processors to use more care in the handling collected data. If a service targets children as one of its audiences, it should be considered directed toward children and appropriate action should be taken to protect the data collected.[262]

E. Challenges Still Lie Ahead

Creating clearer definitions and expectations within the GDPR would promote more consistent compliance with the regulation. However, similar to other areas of law, it is difficult to create a comprehensive regulation that never requires amendment, particularly considering the quickly developing nature of data analytics and information technology. Until the law has been put into action and real-world issues arise, the weaknesses in the regulation are not yet exposed and oftentimes the legislative authorities are not aware of what is inadequately addressed in the regulation. The GDPR could more effectively achieve its goals by looking at the patterns in COPPA and adopting similar definitions for consent, obtaining verifiable consent, by gathering consent through reasonable methods in light of available technology, and by allowing COPPA's over twenty years of experience in child data protection framework to serve as a guideline for children's data protection in the E.U.[263]

While the world of data protection has improved its methods of protecting individuals and their rights to privacy, there are inherent difficulties that tag alongside the idealistic goal of creating a harmonized, effective, and all-encompassing data protection framework.[264] First, technology is advancing at a rapid pace, and the worlds of education, entertainment, and commerce are relying more and more heavily on the Internet and big data services.[265] Like most laws and regulations, a regulation involving technology or data protection will at some point become outdated and in need of revision.[266]

Further, definitions will need to be consistently updated and amended to

---

261. *Id.* at 172-73.

262. *Id.* at 173-74.

263. *Id.* at 191.

264. van der Hof, *supra* note 1, at 437-38.

265. van der Hof, *supra* note 1, at 412-14.

266. Lokke Moerel, *Big Data Protection: How to Make the Draft EU Regulation on Data Protection Future Proof*, TILBURG UNIVERSITY 13 (Feb. 2014).

cover the appropriate technological advancements and changing online environment in this ever-increasingly data-driven world. In the US, the COPPA amended its definitions and added new terms to the child protection framework 15 years after its initial enactment, and it will likely face amendments in the coming years.[267] The cost of compliance with these types of regulations can be significant for those in the online service and tech industries, and those costs can deter people from developing or supporting innovative new tech ideas and learning programs for children.[268] Enforcement of these regulations comes at a cost, too, requiring additional efforts and resources to be put toward the movement from the relevant, overseeing authorities.[269]

Most data protection guidelines and recommendations recognize the importance of balancing the risks to safety and privacy online with the opportunities and freedom of expression that engaging online offers.[270] Many protection frameworks have implemented a child's rights to special protective measures, although it is valuable to take precaution that the concerns associated with children engaging online do not overpower the beneficial ways in which the Internet provides opportunity for children.[271]

The Internet and digital technologies have encouraged creativity and free expression worldwide and have provided enriching opportunities for youth.[272] Protecting children in the online world is an important part of creating a safe environment in which children can be connected to meaningful, age-appropriate content and the world around them. It is also important, however, to ensure that children can continue to experience and engage in the vast array of online activities that connect them to other learning experiences, cultural exploration, or artful expression that they may not otherwise be able to access.

While protecting children online is a complicated venture, more black and white options for protection, like a full age-block (e.g., a website prompts a user to enter a birthdate, and if a birthdate indicates the user is below a certain age, the user will not be able to access the site) may not promote children's access to beneficial online experiences.[273] Further, these methods may not be effective

---

267. FTC Children's Online Privacy Protection Rule, 16 C.F.R. § 312.1 (2013), https://www.ftc.gov/system/files/2012-31341.pdf [https://perma.cc/LRB3-QPFT].

268. Interview with Meaghan Zore, Professor of Law Indiana University Robert H. McKinney School of Law, in Indianapolis, Ind. (Jan. 23, 2019).

269. Beata A. Safari, *Intangible Privacy Rights: How Europe's GDPR Will Set a New Global Standard for Personal Data Protection*, 47 SETON HALL L. REV. 809, 825 (2017).

270. Sonia Livingstone, John Carr & Jasmina Byrne, *One in Three: Internet Governance and Children's Rights*, GLOBAL COMMISSION ON INTERNET GOVERNANCE No. 22, 5 (November 2015), https://www.cigionline.org/sites/default/files/no22_2.pdf [https://perma.cc/P42C-FXJH].

271. *Id*.

272. *The State of the World's Children 2017: Children in a Digital World*, UNICEF: FOR EVERY CHILD, 9 (December 2017), https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf [https://perma.cc/K6ED-L2HC].

273. Macenaite & Kosta, *supra* note 17, at 174-75.

because privacy protection also involves human factors.[274] Even where developers have complied with the relevant data protection laws, children continue to find workarounds, like creating fake parental accounts, lying about their age, or otherwise spoofing systems to bypass age verification or parental consent systems.[275]

Although obtaining parental consent to process a child's data may be complicated for some web services, it is a method of lawful processing through which children can continue to use the online web without undue restrictions. Those involved in data collection and protection have concerns about the costs of compliance with the current data protection regulations, claiming that such strict regulations impose undue strain upon the web services or application developers.[276] They argue that the restrictions imposed by the regulations effectively chase off any monetization opportunities for the web developers and therefore decrease the incentive to create new, engaging, and educational content for children.[277] While these concerns are legitimate, they do not outweigh the importance of keeping data protection at the top of the agenda as technology, information systems, and web-based services continue to develop and increasingly intertwine with daily life.

V. CONCLUSION

Data privacy and protection is a steadily increasing area of concern and focus in the modern tech and data-driven world.[278] Despite the data protection frameworks in place, high percentages of children are reported to regularly use online services directed toward adults, meaning that children frequently access web services that do not render appropriate data protection.[279] Addressing issues within the GDPR that relate to the privacy rights and protection of children, like age of consent for processing, unclear terms like "reasonable efforts" and "verified consent," or exactly what types of services are considered "directed toward children" would help ensure that proper measures for protecting children's privacy online are taken.

While the GDPR has made significant improvements to data privacy regulations in the E.U., there are areas of the regulation that, with clarification and revision, could more successfully harmonize data protection regulations for

---

274. *Id*. at 150.

275. Ilaria Liccardi, et al., *Can apps play by the COPPA Rules?*, 2014 TWELFTH ANNUAL CONFERENCE ON PRIVACY, SECURITY AND TRUST, 3, 9 (2014).

276. Children's Online Privacy Protection Rule, 16 C.F.R. § 312 (2013).

277. *Id*.

278. van der Hof, *supra* note 1, at 444-45.

279. Livingstone, Carr & Byrne, *supra* note 268 at 3. *See also* Livingstone, *supra* note 3, n.10 ("Consider, for example, the top 10 sites visited by six- to 14-year-olds in the United Kingdom in 2013: 63 percent visited Google, 40 percent YouTube, 34 percent the BBC, 27 percent Facebook, 21 percent Yahoo, 17 percent Disney, 17 percent Wikipedia, 16 percent Amazon, 16 percent MSN and 15 percent eBay. . . .").

data subjects in the E.U. Further, the GDPR could provide stronger and more effective protections for children in the online world by incorporating some ideas from the framework for children's data protection in the U.S.

First, the GDPR should implement a uniform age for all European Union countries at which children are able to provide consent for the processing of their own data. Having a uniform age of consent for data processing would help eliminate challenges currently faced by international online services and would help harmonize the regulation of children's data protection. The GDPR is a complex regulatory system designed to help provide individuals with greater privacy rights and to provide companies and processors with clearer guidelines for processing personal data, and implementing a uniform age of consent would eliminate unnecessary challenges currently experienced by the lack of a consistent age requirement throughout the E.U.[280]

Second, the current privacy regulations in the European Union would be strengthened by more clearly delineating the definitions and expectations behind several key aspects of the regulation. Providing more explicit examples of appropriate methods for obtaining verifiable parental consent and incorporating a full prohibition on processing children's data where parental consent has not been obtained would better promote the protection of children online. Further, more clearly defining what constitutes a web service offered "directly to children" may eliminate confusion as to what services need to comply with the child-related portions of the regulation.

Third, online services and E.U. data subjects alike would benefit from stronger and more consistent methods of enforcement of the GDPR.

Youth under the age of 18 use the Internet at the same frequency as the rest of the world's adult population, yet the Internet and data privacy efforts have developed primarily with adult users in mind.[281] Protecting the personal data and privacy rights of adults and children alike is an increasingly important part of the modern, data-driven world.[282]

The world of data privacy and protection has taken many steps in the right direction, although many improvements remain to be made.[283] There are technologies that will be developed in the future that would be difficult to fathom

---

280. Milda MaCenaite, *supra* note 46. *See also* Michael Monajemi, *Privacy Regulation in the Age of Biometrics that Deal with a New World Order of Information*, 25 U. MIAMI INT'L & COMP. L. REV. 371, 379 (2018); Sonia Livingstone, *supra* note 229.

281. Livingstone, Carr & Byrne, *supra* note 270 1, 7. *See also The State of the World's Children 2017: Children in a Digital World*, UNICEF: FOR EVERY CHILD at 1 (December 2017), https://www.unicef.org/publications/files/SOWC_2017_ENG_WEB.pdf [https://perma.cc/UK9J-4WCS].

282. *Children and the Internet*, INTERNET SOCIETY (Nov. 23, 2018), https://www.internetsociety.org/resources/doc/2012/children-and-the-internet/ [https://perma.cc/VFV6-N28Q]. *See generally: Children and Media Tips from the American Academy of Pediatrics*, AMERICAN ACADEMY OF PEDIATRICS (May 1, 2018), https://www.aap.org/en-us/about-the-aap/aap-press-room/news-features-and-safety-tips/Pages/Children-and-Media- Tips.aspx.

283. van der Hof, *supra* note 1, 437-38.

now, and there will be ways in which data and technology will continue to change the way the world communicates and operates.[284] For example, Facebook was launched 15 years ago in 2007, and now Facebook connects over 2.2 billion active monthly users with the world around them.[285] A crucial part of developing and maintaining effective data protection and privacy frameworks is adaptability.[286]

The GDPR has a strong start from the Data Protection Directive, and it has taken measures to provide individuals with stronger protections and control over their privacy rights and personal data.[287] The Regulation has recognized that children warrant special protections in the online world and has implemented new protections for children that provide a solid foundation for developing effective methods to enhance their protection online.[288] Every regulatory initiative has a starting point, and the GDPR has laid strong groundwork for protecting individual's privacy rights in the ever-evolving technological industry. With continued focus on strengthening the privacy of individuals in today's data-driven world, the GDPR will be able to more effectively protect individuals, their data rights and their rights to privacy.

---

284. Moerel, *supra* note 266.

285. *Most popular social networks worldwide as of October 2018, ranked by number of active users (in millions)*, STATISTA: THE STATISTICS PORTAL (Oct. 2018), https://www.statista.com/statistics/272014/global-social-networks- ranked-by-number-of-users/ [https://perma.cc/4498-LDPM].

286. Macenaite & Kosta, *supra* note 17, at 191.

287. Sebastian, *supra* note 31 at 222.

288. Article 29 Data Protection Working Party, *Guidelines on Consent under Regulation 2016/679*, 17/EN WP259 at 22, § 7.1 (Nov. 28, 2017).