Encryption as a safeguard for Human Dignity: An exploration of the link between Privacy and Human Dignity

"These examples and many others demonstrate an alarming trend whereby the privacy and dignity of our citizens is being whittled away by sometimes imperceptible steps. Taken individually, each step may be of little consequence. But when viewed as a whole, there begins to emerge a society quite unlike any we have seen -- a society in which government may intrude into the secret regions of man's life at will." – William O. Douglas (Associate Justice of the Supreme Court of the United States)

INTRODUCTION

The rapid expansion of the Internet over the past decade has led to increased digital activity by individuals as well as a proliferation of services ranging from ecommerce sites to social media platforms. More recently, unforeseen events like the present COVID-19 pandemic have further contributed to a rise in the use of online services such as video conferencing and streaming [1,2]. Expectedly, individuals are increasingly generating and exchanging content, including private information, over the Internet. These factors have inevitably led to an exponential growth of information on the Internet; it is claimed that in 2020 individuals produced 2.5 quintillion[i] bytes of data daily while 463 exabytes[ii] of data is projected to be generated by 2025[3]. Considering the vast amounts of information generated, exchanged, and hosted on the Internet, individuals rely on mechanisms like encryption to protect their privacy by safeguarding their digital or Internet-based activities.

Encryption enables individuals to conduct secure and confidential communications and transactions and prevents unauthorized access or intrusions to individuals' internet-enabled devices. Recent demands by state actors to technology companies to circumvent encryption controls by providing them with "exceptional access"[4–6] however threaten the privacy afforded individuals by these mechanisms. As privacy is recognized as a fundamental human right,[7,8] requests by governments to undermine encryption can be regarded as an attempt to violate individuals' dignity.[9,10] With plans underway to get more people on the Internet by 2030,[11] it is imperative that individuals can safely and securely perform digital activities without being subject to the effects of undermined encryption. This paper focuses on exploring the link between privacy and human dignity, and how redefining privacy through the lens of human dignity may strengthen the case for encryption mechanisms.

[i] A quintillion has 18 zeroes (1,000,000,000,000,000,000)

[ii] 1 exabyte roughly equals 1 billion gigabytes (GB)

MAPPING OF FOUND EVIDENCE

Search Results

The search was conducted on Scopus, Web of Science and Google between December 2020 and January 2021 and centered on terms reflecting the paper's topic. These included "encryption", "privacy", "human rights", and "dignity" and their possible derivatives. The methodology adopted in executing the search is described in detail in Annex A.1. To obtain an understanding of existing scholarly work relating to the benefits and/or disbenefits of encryption and affected stakeholders, the evidence selected predominantly comprises journal articles. Summarized below are the search results and scale of exclusions.

Table 1: Summary of search results

Source	Initial Search Results	Final Search Results	Document Type	Selected Evidence
Scopus	1,749	231	Article (107)	**2**
			Conference Paper (77)	**-**
			Book Chapter (19)	**-**
			Review (14)	**-**
			Book (7)	**-**
			Conference Review (3)	**-**
			Editorial (2)	**-**
			Short Survey (2)	**-**
Web of Science[iii]	89	89	Article (61)	**2**
			Proceedings Paper (16)	**-**
			Article; Book Chapter (5)	**-**
			Review (4)	**-**
			Article; Proceedings Paper (2)	**-**
			Editorial Material (1)	**-**
Google	~4 million pages	~4 million pages	Discussion Paper	**1**

Table 2: Scale of excluded results

Source	Scale of Exclusions	Rationale
Scopus	87%	To obtain a manageable range of returns. Additionally, the focus was less on encryption technologies and functionalities, which most of the results indicate.
Web of Science	0%	No exclusions were made to the search results to avoid inadvertently omitting salient evidence.
Google	~99%	The search was focused on finding one piece of evidence that was legitimate, salient and credible.

[iii] Due to how the native analysis function on Web of Science categorized the results, there were instances of the same papers being grouped into multiple categories. This resulted in a higher count than the actual number of results (96 vs 89).

The initial search on Scopus using identified key words and phrases (including wild cards) from the problem statement (encrypt*, priva*, "human dignity") yielded a single result; a book which is only available in print and thus inaccessible. Expanding the search criteria using synonyms representative of the key words and phrases and applying the period filter[iv] resulted in 1,749 returns. These were further filtered with the condition "encrypt*" OR "dignity" to 231 returns; of which two articles were eventually selected as evidence. The chart (right) illustrates the distribution of returns with articles representing the largest portion (46.3%).

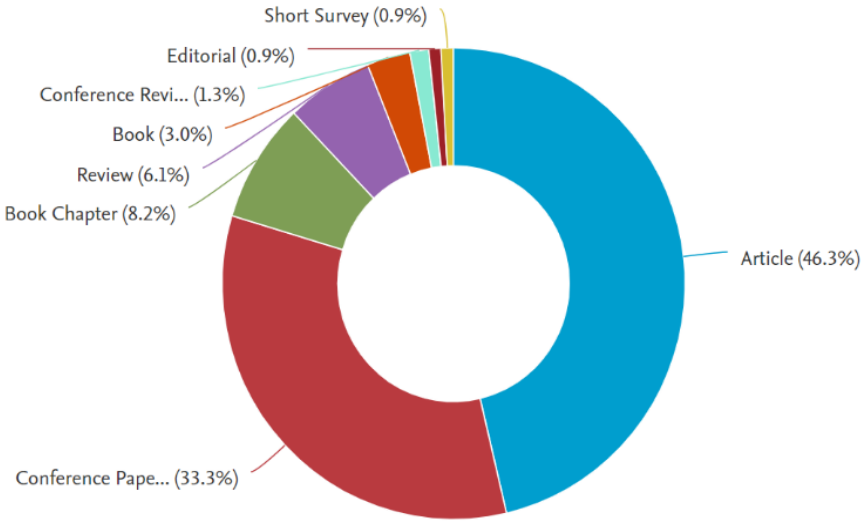

Figure 1: Scopus Results – Documents by type

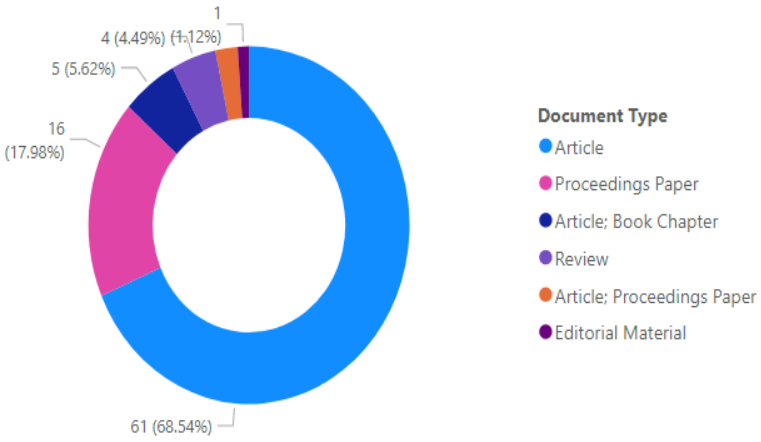

Figure 2: Web of Science Results – Documents by type

Similar terms were used for the Web of Science searches; the initial search yielded no returns while the expanded search returned 89 results. Given the relatively low search results, additional filtering rules were not applied. Like the Scopus findings, articles represent a significant part (69%) of the returns as depicted in the chart to the left.

In conducting the Google search, the focus was on grey literature published by academia, think tanks or privacy advocacy organizations. The search employed the terms "human dignity", "privacy", and "encryption" and focused on results from 2000 to 2020.

[iv] Table of defined search terms and period filters are detailed in Annex A.1.

SYNTHESIS OF FOUND EVIDENCE

Given that online privacy and security mechanisms are critical to a wide scope of stakeholder groups (individuals and organizations), it was essential to identify evidence that highlights these themes from varied perspectives. Consequently, the five papers[v] selected portray viewpoints from human rights organizations, legal practitioners, technologists, and researchers. All five papers [12–15,10] broadly recognize that individuals have a right to privacy with each highlighting a variety of avenues for assessing privacy-related concerns. Furthermore, four papers reflect a sampling of geographical contexts while the fifth paper recognizes privacy through the lens of child rights and provides an opportunity to consider how privacy impacts a particularly vulnerable class of people.[16] Identified themes across the papers are discussed in the rest of this section.

Privacy Definitions

Despite privacy being acknowledged under international law as a fundamental human right,[17] an immediate and consistent theme across the five papers is a difficulty in the clear definition of privacy and what it entails. Four of the papers also attempt to establish a relationship with human dignity while the fifth paper neither mentions any such connection nor expounds on a definition of privacy.

One of the papers provides three related concepts in defining privacy; decisional privacy, informational privacy and physical privacy.[10] Data protection which is linked to informational privacy[18,19] is also mentioned in two of the four papers as a key determinant for conceptualizing a more concrete definition for privacy. Both papers however adopt contrasting positions. While one paper situates this definition alongside other rights and within the context of emerging technologies [12], the other paper adopts an economic position alluding to Singapore's intentions of becoming "a leader in the region for data storage and processing". [15] In addition, they both represent separate ideologies as the former reflects an European rights-based view on privacy [20], whereas the latter presents an economically-inspired Asian outlook. [15]

The fourth paper engages privacy from a markedly different standpoint. Rather than employ the traditional approach of rights infringement or non-interference [21], this paper examines the non-domination principle in advancing privacy rights. It references the

---

[v] Privacy, data protection and emerging sciences and technologies
http://www.tandfonline.com/doi/abs/10.1080/13511611003791182
No Backdoors: Investigating the Dutch Standpoint on Encryption
http://onlinelibrary.wiley.com/doi/abs/10.1002/poi3.233
A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle
http://www.sciencedirect.com/science/article/pii/S0267364917303849
After Privacy: The Rise of Facebook, the Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012
http://www.ssrn.com/abstract=2255274
UNICEF_CRB_Digital_World_Series_PRIVACY
https://sites.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

European Court of Human Rights (ECtHR) which in the face of "complex data-driven cases in which concrete damage and individual harm are difficult to substantiate"[14] has recently adopted this strategy to decide cases of this nature. The argument for non-domination is premised on republicanism and it espouses the notion of individuals being free from subjugation and arbitrary interference by external entities. [22] In adopting this position, the ECtHR is concerned with safeguarding against "the arbitrary use of power"[14] by state actors and big technology companies in online privacy disputes.

Data Protection and Encryption

Although data protection is generally mentioned in the five papers, only two of the papers explicitly mention encryption. One paper presents conflicting views on encryption; while encryption technologies are useful in protecting children's privacy online, they also provide "safe spaces" enabling perpetrators to commit crimes like creating and storing images depicting child sexual abuse (IDCSA). [23] This undoubtedly presents a challenge to both child rights activists and investigators in combating crimes of this nature. It also raises the question of identifying the exact stakeholders for whom encryption is both legitimate and salient in addressing online crimes against children. [24] Expectedly, this presents a need for nuanced approaches to encryption rather than inflexible strategies.

The second paper analyzes the strategy adopted by the Netherlands in deciding its stance on encryption. Against a backdrop of ongoing debates on encryption and backdoors, the paper provides a justification for encryption through the lenses of economics, national security and privacy. [13] The economics lens mirrors the position expressed in one of the three papers that do not mention encryption. While this paper considers data protection necessary for enabling trust in Singaporean institutions and integration with global networks [15], the Netherlands paper argues that encryption provides the foundational trust required to drive economic activities like online banking and shopping. [13] It is immediately evident that encryption facilitates trust in "borderless" transactions. [25,26]

Of the other three papers that solely mention data protection, one paper rationalizes the application of non-domination to regulate data collection and storage processes in Europe. As data are used in decision-making activities that impact societies, the non-domination principle will be useful in clarifying the role of regulation in mediating power imbalances involving citizens, states and technology companies. [27] While the last paper which excludes encryption acknowledges that data protection provides a more encompassing approach and definition to privacy, it does not indicate inequalities in the relationships between data subjects (i.e. individuals) and data processors/controllers. [28] Instead, it spotlights the European Union funded Privacy and Emerging Sciences and Technologies (PRESCIENT) project which seeks to deliver "a new privacy framework for privacy and ethical considerations" necessitated by emerging technologies [12]. The Privacy and Ethical Impact Assessment (P+EIA) Framework, a key deliverable of the PRESCIENT

project however includes “asymmetries of power”[vi] and “trust”[vii] as ethical and social issues to contemplate in developing new technologies. [29]

Privacy and Human Dignity

As previously stated in the Privacy Definitions section, four papers imply a possible connection between privacy and human dignity albeit in varying degrees of detail. The one paper (the Netherlands one) which does not mention dignity, however, suggests in its analysis of encryption through the privacy lens, that compromised encryption mechanisms are injurious to human rights. [30] It also reflects how the non-domination principle is violated by citing instances where state actors have exploited information to victimize citizens. [13,31]

Of the four papers that indicate a link between privacy and human dignity, the first one mentions human dignity once in the abstract section and claims it is underpinned by privacy. However, the previously mentioned deliverable from the PRESCIENT project holds some promise for preserving human dignity. In the second paper, privacy is described as a subjective right exercised in the protection of one’s “personal interests such as relating to human dignity”. [14] It also deems non-interference unsuitable in preventing exploitation in disproportionate social interactions (for instance, between state and citizen) [14], given that the opportunity to do so still exists. [32] Nonetheless, the paper recognizes that when viewed through the lens of republicanism, the non-domination principle may be helpful in protecting human dignity and autonomy. Consequently, the individual’s right to privacy and dignity is upheld. [33]

The third paper which refers to human dignity does so only to compare the definitions of privacy in both the European and United States contexts. While the European meaning is rooted in protecting “the personal honor or dignity of individuals”, [15] the American outlook promotes privacy as “protection from external interference”. [15] It is against these apparent dichotomous inconsistencies [20] that the paper considers present definitions of privacy as insufficient in aligning with the digital age.

Finally, the last (i.e. fourth paper) mentions privacy as being “at the heart of the most basic understandings of human dignity”[10] but does not provide additional details. However, since the paper discusses vulnerabilities that children are exposed to online, it may be said that intrusive actions like IDCSA and brokerage of children’s personal data which demonstrate a significantly imbalanced power dynamic, are harmful to children’s dignity. [34,35]

[vi] Asks the question “Will the project or technology enhance the power of some at the expense of others?”

[vii] Asks the questions “Will the technology or project impact trust and/or social cohesion? Will groups or individuals believe they are not trusted by others, especially those who are in a stronger position of power?”

CONCLUSION

To enable a more nuanced conversation on encryption, this paper has attempted to establish a connection between privacy and human dignity, and how this link is affected by weakened encryption mechanisms. An apparent issue is the need for a clear definition of privacy and how it relates to diverse stakeholders (individuals, organizations, governments etc.). Rather than view dignity as an offshoot of privacy, it is suggested that defining privacy within the frame of human dignity[viii] would be beneficial to addressing stakeholder concerns around encryption. As has been noted with the European and American contexts, the understanding of privacy[36] has largely influenced both entities' approach to data protection practices. Thus, constructing narratives to reflect the "inviolate personality"[37] that is definitive of human dignity which do not also alienate or marginalize any stakeholder group may be helpful in resolving the encryption debate. [38,39] This is particularly significant for child rights activists who contend with the dual challenge of balancing the benefits and risks of encryption. Conversely, there is also a need to situate these definitions within jurisdictional contexts.

The non-domination principle also presents a possible avenue to redefine privacy from the viewpoint that individuals should be protected from arbitrary interferences by more powerful actors. [40,41]

Lastly, a multi-stakeholder strategy may contribute to advancing policy discussions on encryption. The Netherlands paper attributes the Dutch's government decision not to undermine encryption through the implementation of backdoors, to a deliberative process with state departments, technical and intelligence experts and civil society. [13] Although this strategy proved valuable in this instance, there is a concern that multi-stakeholder deliberations may serve to reinforce group think or biases [42] and may prolong the policy making process.

[viii] This paper aligns with the Center for Bioethics & Human Dignity's definition of human dignity which recognizes it as "an inherent quality in all humans" by which human beings "are worthy of respect".

REFERENCE LIST

1. Why the coronavirus lockdown is making the internet stronger than ever [Internet]. MIT Technology Review. [cited 2021 Jan 12]. Available from: https://www.technologyreview.com/2020/04/07/998552/why-the-coronavirus-lockdown-is-making-the-internet-better-than-ever/

2. Kende - Impact of COVID-19 on the Internet Ecosystem in th.pdf [Internet]. [cited 2021 Jan 12]. Available from: https://www.internetsociety.org/wp-content/uploads/2020/11/Impact-Covid-19-Internet-Ecosystem-MENA_EN.pdf

3. How Much Data Is Created Every Day in 2020? [You'll be shocked!] [Internet]. TechJury. 2020 [cited 2021 Jan 12]. Available from: https://techjury.net/blog/how-much-data-is-created-every-day/

4. Schulz and van Hoboken - 2016 - Human rights and encryption.pdf [Internet]. [cited 2021 Jan 12]. Available from: https://www.ivir.nl/publicaties/download/human_rights_and_encryption.pdf

5. Ruiz D. There is No Middle Ground on Encryption [Internet]. Electronic Frontier Foundation. 2018 [cited 2021 Jan 12]. Available from: https://www.eff.org/deeplinks/2018/05/there-no-middle-ground-encryption

6. Factsheet: Encryption - Home Office in the media [Internet]. [cited 2021 Jan 12]. Available from: https://homeofficemedia.blog.gov.uk/2019/11/05/factsheet-encryption/

7. udhr_booklet_en_web.pdf [Internet]. [cited 2021 Jan 12]. Available from: https://www.un.org/en/udhrbook/pdf/udhr_booklet_en_web.pdf

8. OHCHR | International Covenant on Civil and Political Rights [Internet]. [cited 2021 Jan 12]. Available from: https://www.ohchr.org/en/professionalinterest/pages/ccpr.aspx

9. Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development [Internet]. Koninklijke Brill NV; [cited 2021 Jan 13]. Available from: https://primarysources.brillonline.com/browse/human-rights-documents-online/promotion-and-protection-of-all-human-rights-civil-political-economic-social-and-cultural-rights-including-the-right-to-development;hrdhrd99702016149

10. UNICEF_CRB_Digital_World_Series_PRIVACY.pdf [Internet]. [cited 2021 Jan 13]. Available from: https://www.unicef.org/csr/files/UNICEF_CRB_Digital_World_Series_PRIVACY.pdf

11. Connecting humanity Assessing investment needs of connecting humanity to the Internet by 2030. :36.

12. Friedewald M, Wright D, Gutwirth S, Mordini E. Privacy, data protection and emerging sciences and technologies: towards a common framework. Innov Eur J Soc Sci Res. 2010 Mar;23(1):61–7.

13. Veen J, Boeke S. No Backdoors: Investigating the Dutch Standpoint on Encryption. Policy Internet. 2020;12(4):503–24.

14. van der Sloot B. A new approach to the right to privacy, or how the European Court of Human Rights embraced the non-domination principle. Comput Law Secur Rev. 2018 Jun 1;34(3):539–49.

15. Chesterman S. After Privacy: The Rise of Facebook, the Fall of Wikileaks, and Singapore's Personal Data Protection Act 2012. SSRN Electron J [Internet]. 2012 [cited 2021 Jan 24]; Available from: http://www.ssrn.com/abstract=2255274

16. Halder D. Children of internet era: A critical analysis of vulnerability of children in the darker sides of social media and WhatsApp. 2015.

17. eng.pdf [Internet]. [cited 2021 Jan 24]. Available from: https://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/eng.pdf

18. Informational privacy, consent and the ••control•• of personal data | Elsevier Enhanced Reader [Internet]. [cited 2021 Jan 24]. Available from: https://reader.elsevier.com/reader/sd/pii/S1363412709000363?token=01A096F9E6F72871082864FCE83442C96ACFC0FAAD543ABF4C8AB77BFCD5CFE303871675E860AC04156B9281A821529C

19. Towards Informational Privacy.pdf.

20. Whitman JQ. The Two Western Cultures of Privacy: Dignity versus Liberty. Yale Law J. 2004;113(6):1151–221.

21. Nielsen MEJ, Landes X. Fighting Status Inequalities: Non-domination vs Non-interference. Public Health Ethics. 2016 Jul;9(2):155–63.

22. Pettit - 1999 - Republicanism.pdf [Internet]. [cited 2021 Jan 24]. Available from: https://oxford.universitypressscholarship.com/view/10.1093/0198296428.001.0001/acprof-9780198296423-chapter-3?print=pdf

23. Combatting those who intentionally access images depicting child sexual abuse on the Internet: A call for a new offence in England and Wales | Elsevier Enhanced Reader [Internet]. [cited 2021 Jan 24]. Available from: https://reader.elsevier.com/reader/sd/pii/S0267364917302042?token=F2F09AF08A34F363273685D2AF20D3F3182DD4C7E59DA7D39AE2AA97090DEFCC82EA76C91AC15386A52630CBA6F2B046

24. Majchrzak A, Markus ML. Methods for Policy Research: Taking Socially Responsible Action [Internet]. 1 Oliver's Yard, 55 City Road London EC1Y 1SP: SAGE Publications, Ltd; 2014 [cited 2021 Jan 23]. Available from: http://methods.sagepub.com/book/methods-for-policy-research-2e/

25. Peikari HR. A Study on the Interrelations between the Security-Related Antecedents of Customers' Online Trust. In: Tenreiro de Magalhães S, Jahankhani H, Hessami AG, editors. Global Security, Safety, and Sustainability [Internet]. Berlin, Heidelberg: Springer Berlin Heidelberg; 2010 [cited 2021 Jan 24]. p. 139–48. (Communications in Computer and

Information Science; vol. 92). Available from: http://link.springer.com/10.1007/978-3-642-15717-2_16

26. Hardy K. Australia's encryption laws: practical need or political strategy? Internet Policy Rev [Internet]. 2020 Aug 27 [cited 2021 Jan 24];9(3). Available from: https://policyreview.info/articles/analysis/australias-encryption-laws-practical-need-or-political-strategy

27. Personal data for decisional purposes in the age of analytics: From an individual to a collective dimension of data protection | Elsevier Enhanced Reader [Internet]. [cited 2021 Jan 24]. Available from: https://reader.elsevier.com/reader/sd/pii/S026736491630028O?token=2B4CC044E063C205C6C1AC83FCF72E99724B8916AF3206B75665473946E817603D50A240155441979972BC276893FCDE

28. Vulnerable data subjects | Elsevier Enhanced Reader [Internet]. [cited 2021 Jan 25]. Available from: https://reader.elsevier.com/reader/sd/pii/S0267364920300200?token=EFCC3DB7108B569F186201965329A59853E74FCF6355653C2CDC583CB1EDF429D7C552FD99BA6C06EF147527006782F1

29. PRESCIENT_Final Report — A Privacy and Ethical Impact Assessment Framework for Emerging Sciences and Technologies.

30. Schulz W, van Hoboken J. Human rights and encryption. United Nations Educational, Scientific, and Cultural Organization; 2016.

31. Kaye-HRC-Report-Encryption-Anonymity.pdf [Internet]. [cited 2021 Jan 25]. Available from: http://www.justsecurity.org/wp-content/uploads/2015/06/Kaye-HRC-Report-Encryption-Anonymity.pdf

32. Pettit P. Republicanism [Internet]. Oxford University Press; 1999 [cited 2021 Jan 25]. Available from: http://www.oxfordscholarship.com/view/10.1093/0198296428.001.0001/acprof-9780198296423

33. Roberts A. A republican account of the value of privacy. Eur J Polit Theory. 2015 Jul 1;14(3):320–44.

34. Xafis V. Why respecting all human beings' privacy matters. J Paediatr Child Health. 2016;52(3):256–7.

35. Kardefelt-Winther D, Day E, Berman G, Witting SK, Bose A. Encryption, Privacy and Children's Right to Protection from Harm. :13.

36. The Polysemy of Privacy.pdf.

37. Warren and Brandeis, "The Right to Privacy" [Internet]. [cited 2021 Jan 25]. Available from: https://groups.csail.mit.edu/mac/classes/6.805/articles/privacy/Privacy_brand_warr2.html

38. Thibodeau PH, Boroditsky L. Metaphors We Think With: The Role of Metaphor in Reasoning. Lauwereyns J, editor. PLoS ONE. 2011 Feb 23;6(2):e16782.

39. Malone E. Stories about ourselves_ How national narratives influence the diffusion of large-scale energy technologies. Soc Sci. 2017;7.

40. Pettit P. Republicanism [Internet]. Oxford University Press; 1999 [cited 2021 Jan 24]. Available from: http://www.oxfordscholarship.com/view/10.1093/0198296428.001.0001/acprof-9780198296423

41. Allen AL. LAW, PRIVACY & TECHNOLOGY COMMENTARY SERIES. 130:9.

42. Stakeholder engagement as a conduit for regulatory legitimacy? [Internet]. [cited 2021 Jan 25]. Available from: https://www-tandfonline-com.libproxy.ucl.ac.uk/doi/epub/10.1080/13501763.2020.1817133?needAccess=true

43. Human Dignity [Internet]. [cited 2021 Jan 17]. Available from: https://cbhd.org/category/issues/human-dignity

44. Policy Brief: Privacy [Internet]. Internet Society. [cited 2021 Jan 17]. Available from: https://www.internetsociety.org/policybriefs/privacy/

45. SEP - Snapshot [Internet]. [cited 2021 Jan 13]. Available from: https://plato.stanford.edu/archives/sum2020/entries/it-privacy/

46. Lewis et al. - 2017 - The effect of encryption on lawful access to commu.pdf [Internet]. [cited 2021 Jan 13]. Available from: https://ec.europa.eu/home-affairs/sites/homeaffairs/files/what-we-do/policies/organized-crime-and-human-trafficking/encryption/csis_study_en.pdf

METHODOLOGY

The factors outlined below were considered in finding, judging, and synthesizing the evidence scoped for this paper:

- **Definitions:** To properly situate the term within the context of this paper, the definition of "human dignity" follows the Center for Bioethics & Human Dignity's philosophy[43] which recognizes it as "an inherent quality in all humans" by which human beings "are worthy of respect". Although, there is presently no universal definition of the word,[10] this paper aligned with the Internet Society to define "privacy" as "the right to determine when, how, and to what extent personal data can be shared with others".[44]
- **Medium/channel:** The Internet was selected as the focal medium because it facilitates a wide range of digital services including platforms and devices (mobile phones, smart speakers, "wearables"[ix] etc.). Further, the Internet is powered by protocols which enable communication and data transfer. The Internet is also referred to as "online" in the main document.
- **Period:** The search was primarily focused on the 20-year period up to 2020 to reflect how the Internet's evolution as well as technology advancements have triggered discussions around encryption and privacy in this time.[45,46]
- **Sources:** Scopus, Web of Science and Google (for grey literature advocating the use of encryption to safeguard privacy) formed the sources of found evidence.

Search Terms and Search Strings

20 search terms were defined along the broad themes of Encryption, Internet, Dignity and Weaken and used for the expanded search on Scopus and the Web of Science. For both the Scopus and Web of Science results, each abstract was analyzed and read to identify any of the relevant terms. Papers that chiefly dwelt on technical implementations of encryption mechanisms were completely excluded.

Table 3: Defined Search Terms

Encryption	Internet	Human Dignity	Weaken
Encrypt*	Interne*	Valu*	Backdoor*
Secur*	Connect*	Respect	"Back door*"
Protect*	Communicat*	Ethic*	"Back-door*"
Confidenti*	Data*	Moral*	Undermin*
	Online	Worth*	
	Web	Priva*	

Scopus search criteria and syntax:

[ix] Wearables – "any kind of electronic device designed to be worn…including jewelry, accessories, medical devices and clothing (or elements of clothing)" [https://searchmobilecomputing.techtarget.com/definition/wearable-technology]

The Scopus search criteria were also filtered with the terms “encrypt*” and “dignity” to ensure that the returns included papers salient to the topic. This compensated for the possibility of not capturing relevant evidence if only one of both filter terms was used, as some of the search returns may not have explicitly contained both terms. The built-in analysis function on Scopus was also used to determine the distribution of results across the “Document Type” category.

Search string:

((((((TITLE-ABS-KEY (encrypt* OR secur* OR protect* OR confidenti*) AND ALL (interne* OR connect* OR communicat* OR data OR online OR web) AND TITLE-ABS-KEY (dignity OR valu* OR respect OR ethic* OR moral* OR worth* OR priva*) AND TITLE-ABS-KEY (backdoor* OR "back-door*" OR "back door*" OR undermin*)) AND PUBYEAR > 1999 AND PUBYEAR < 2021)))) AND ((**encrypt***) OR (**dignity**)))

Web of Science criteria and search syntax:

The search criteria and syntax employed on Web of Science largely mirrored the Scopus approach with the exceptions being excluding the “confidenti*” term and leaving the results unfiltered. This was to allow for a different outcome than Scopus and avert the likelihood of missing relevant evidence, given the low number of results. As the Web of Science analysis function did not reveal a true representation of the results (see Table 3),[x] the data were exported and further analyzed using Microsoft Excel and PowerBI to ensure a more accurate categorization.

Table 3: Web of Science Results Analysis

Select	Field: Document Types	Record Count	% of 89	Bar Chart
☐	ARTICLE	68	76.404 %	
☐	PROCEEDINGS PAPER	18	20.225 %	
☐	BOOK CHAPTER	5	5.618 %	
☐	REVIEW	4	4.494 %	
☐	EDITORIAL MATERIAL	1	1.124 %	

Search string:

TS = (encrypt* OR secur* OR protect*) AND ALL = (interne* OR connect* OR communicat* OR data OR online OR web) AND TS = (priva*) AND TS = (dignity OR valu* OR respect OR ethic* OR moral* OR worth*) AND TS = (backdoor* OR "back-door*" OR "back door*" OR undermin*)

Google criteria and search syntax:

The search executed on Google entailed using the words “human dignity”, “encryption” and “privacy” which led to selecting a discussion paper reflecting the perspective of a

[x] Due to how the native analysis function on Web of Science categorized the results, there were instances of the same papers being grouped into multiple categories. This resulted in a higher count than the actual number of results (96 vs 89).

global human-rights organization. This paper was picked because it examines contrasting views on how encryption affects children's digital rights and online privacy.

Search string:

human dignity privacy encryption - Google Search

REFLEXIVE ANALYSIS

Prior to this assessment, I had not critically considered the impact of encryption from a socio-technical perspective. This might seem slightly at odds with my Computer Science background, but I had only previously considered it with respect to protecting my devices with strong passwords, performing online transactions securely and a general understanding that my communications on media platforms like WhatsApp were confidential. This assessment and the learnings from the course have challenged me to contemplate issues such as these from a variety of perspectives. In truth, this is partly my reason for selecting this MPA programme.

While this assessment may eventually respond to a specific real client's needs (in this case, the Internet Society), recognizing that the Internet is a massive borderless space was helpful in understanding that encryption is an issue which affects anyone connected to the Internet. It is also not too far-fetched to assume this extends to the offline community by way of second-order effects like misinformation and fake news. This influenced my decision to not limit the target of this paper to a specific class of individuals. I however decided to include a piece of evidence that reviews the impact of encryption on children to show a human side to the paper.

Framing the "right" research question was quite challenging, and I think this may have impacted my search strategy and eventual results. For instance, over 80% of my Scopus results were biased towards technical implementations of encryption. Deciding what classifies as salient and credible evidence also proved to be a not quite straightforward activity. I also wonder about the implication of using evidence that has either low or no citations. Generally, the evidence gathering and judging aspect was the most tricky part of the assessment for me.