



# INDIAN JOURNAL OF LEGAL AFFAIRS AND RESEARCH

VOLUME 3 ISSUE 1

Peer-reviewed, open-access, refereed journal

**IJLAR**

+91 70421 48991  
editor@ijlar.com  
www.ijlar.com

## **DISCLAIMER**

The views and opinions expressed in the articles published in the Indian Journal of Legal Affairs and Research are those of the respective authors and do not necessarily reflect the official policy or position of the IJLAR, its editorial board, or its affiliated institutions. The IJLAR assumes no responsibility for any errors or omissions in the content of the journal. The information provided in this journal is for general informational purposes only and should not be construed as legal advice. Readers are encouraged to seek professional legal counsel for specific legal issues. The IJLAR and its affiliates shall not be liable for any loss or damage arising from the use of the information contained in this journal.

## **Introduction**

Welcome to the Indian Journal of Legal Affairs and Research (IJLAR), a distinguished platform dedicated to the dissemination of comprehensive legal scholarship and academic research. Our mission is to foster an environment where legal professionals, academics, and students can collaborate and contribute to the evolving discourse in the field of law. We strive to publish high-quality, peer-reviewed articles that provide insightful analysis, innovative perspectives, and practical solutions to contemporary legal challenges. The IJAR is committed to advancing legal knowledge and practice by bridging the gap between theory and practice.

## **Preface**

The Indian Journal of Legal Affairs and Research is a testament to our unwavering commitment to excellence in legal scholarship. This volume presents a curated selection of articles that reflect the diverse and dynamic nature of legal studies today. Our contributors, ranging from esteemed legal scholars to emerging academics, bring forward a rich tapestry of insights that address critical legal issues and offer novel contributions to the field. We are grateful to our editorial board, reviewers, and authors for their dedication and hard work, which have made this publication possible. It is our hope that this journal will serve as a valuable resource for researchers, practitioners, and policymakers, and will inspire further inquiry and debate within the legal community.

## **Description**

The Indian Journal of Legal Affairs and Research is an academic journal that publishes peer-reviewed articles on a wide range of legal topics. Each issue is designed to provide a platform for legal scholars, practitioners, and students to share their research findings, theoretical explorations, and practical insights. Our journal covers various branches of law, including but not limited to constitutional law, international law, criminal law, commercial law, human rights, and environmental law. We are dedicated to ensuring that the articles published in our journal adhere to the highest standards of academic rigor and contribute meaningfully to the understanding and development of legal theories and practices.

## **"THREATS TO PRIVACY: DEEPFAKES, 3D AVATARS, AND THE FUTURE OF HUMAN DIGNITY"**

AUTHORED BY - ROSHAN KUMAR GIRI & ANKUR SINGH

### **Abstract:-**

Now, in an era of technology, nobody is left without using electronic devices. There are many developments, from the awakening of the bad to the sleep of our complete life, running by science and technology. Hence, it is crucial to consider how individuals can safeguard their data and how they can permanently destroy it. Recently, many companies have started selling the data of their customers, whether you are a minor or a major customer. But when you use any device, first of all, you have to log in. Without that, you cannot avail yourself of the services of particular websites or any other thing that is based on technology. Let us assume that you can enter an incorrect name, age, or any other information, but your email address or personal phone number must be entered correctly. Otherwise, you will not receive the OTP on your mobile device; as a result, you will not be able to access their services. They say that their business wants to look into it to see if you are a real customer or not. After putting in and filling out the data, most of your things are deduced from your email. The company can understand your data and emotions as well as your lifestyle—what you are most likely to eat and what you are most likely to wear—because every time you put in your email to log in, data analytics in the company measures you every second, and also what type of device you are operating, as well as your family. All the information is there. Now, the most important question that arises here is: when you fill out the data and then log out, normal people understand that the data cannot be used by companies once again, but it is not the truth because it is still stored by the company. Recently, Meta used to make 3D (META VERSE -related devices with which you can fill in and watch your ancestors. But how is it possible? One person is no more, yet others can use the data of that deceased person. And because a deceased person has the right to die, or there is still the right to die peacefully. The second question that arises here is: if any company uses our ancestral data to convert and show it to you in the form of video or anything else. I am asking you, with that data of our ancestral data

and without my permission, how can the company use and sell to me my parents' data, which was purchased by me? It is really a complicated problem and also violates our constitutional rights, Article 14 and Article 21 of the Constitution as well. My question is, what are the remedies and what about the justice who passed away how they and their family avail the justice? Many companies do that; what remedies will be available to them?

### **Introduction-**

Today, a large part of our lives takes place online, but what happens to our digital presence after we die? Even after death, our personal data remains, and through AI, people can now engage with digital representations of those who have passed away. In the future, there may be more inactive accounts than active ones on sites like Facebook. Over the next thirty years, almost two billion people will die, leaving behind a massive digital footprint. Whoever has control over this data will essentially control our digital past, which could have major political and social implications. Carl Öhman suggests that we need to quickly reconsider how we handle digital remains and collaborate to safeguard our collective digital legacy before it's too late.

“Who controls the past controls the future: who controls the present controls the past.” —

*George Orwell, 1984*

In the digital era, social media platforms like Facebook now provide features such as memorialization and account removal following a user's death. However, account deletion usually does not lead to the total removal of personal information. In the developing metaverse era, this raises major concerns about whether digital identities will ever truly vanish or simply be kept in new virtual formats. The issue is made worse in societies with low levels of digital knowledge. In India, literacy is frequently defined as the ability to read or write one's name, but many people who are considered literate lack the ability to understand complicated digital interfaces, privacy agreements, and consent procedures. As a result, a significant number of users are unable to make well-informed choices about what happens to their data in the future.

If Facebook's growth reaches a steady point, the number of deceased users could surpass that of living users by the 2060s; if the platform continues to expand, it may be handling the data of

billions of deceased users by the end of this century. At such a large scale, business interests will decide which data is kept and which is deleted. Since digital data can be erased quickly, remembrance will depend not on human dignity but on profit, which could lead to the removal of marginalized communities from digital history.

Now many companies accumulate and collect data, and then sell that data to other companies. More than ten years have passed since 1) Edward Snowden revealed how companies such as Facebook, Google, and Apple shared user data with the U.S. National Security Agency. In response to growing public worries, important data protection laws like the 1) General Data Protection Regulation (GDPR) and the California Consumer Privacy Act (CCPA) were introduced to strengthen consumer rights and regulate how corporations handle data. Although these laws offer substantial safeguards, many individuals still take personal measures to protect their information, such as managing their own email and other digital services to avoid being monitored by companies.

When it comes to data collection, the focus is usually on consumer-facing platforms like Gmail, Amazon, Facebook, Twitter, and LinkedIn. However, far less attention is paid to business-to-business (B2B) companies that operate behind the scenes. These companies collect and process large amounts of personal information, including names, addresses, phone numbers, banking details, and purchase histories. Using tools like marketing software, data analysis platforms, and customer relationship management systems, B2B firms supply data to consumer-oriented platforms. This hidden data network plays a major role in shaping online experiences, yet it remains largely invisible to users, raising serious concerns about transparency, consent, and accountability in modern data management systems.

And there following companies - Many large, yet less well-known companies play a significant role in gathering and handling personal data. Adobe collects detailed information about user behavior through its Marketing Cloud, creating consumer profiles for advertising purposes. Salesforce holds massive volumes of customer data for airlines, retailers, and other businesses, making it a key center for digital commerce data. Acxiom, a major data broker, connects personal details with online identifiers and sells identity graphs to other companies. Ad networks like

Xander gather browsing history and demographic data to allow targeted advertising across various websites.

Website platforms such as Shopify, Wix, and Squarespace monitor user activity and purchasing behavior to enhance their services and may support future advertising strategies. Customer Data Platforms (CDPs) bring together data from various sources to customize content and marketing efforts. Google Analytics tracks website activity and can associate it with individual identities within Google's network. Content Delivery Networks like Cloudflare observe IP addresses and location data for most web traffic. Credit agencies such as Experian collect detailed financial records. Lastly, Internet service providers like Verizon and Comcast access browsing metadata and use it to assist advertising companies. Collectively, these companies create a hidden data economy that influences digital life, even though it remains largely unnoticed by innocent users.

- 1- <https://gdpr-info.eu>
- 2- <https://oag.ca.gov/privacy/ccpa>
- 3- <https://news.ycombinator.com/item?id=25481465> 4- <https://www.adobe.com>
- 5- <https://www.salesforce.com/in/?ir=1>
- 6- <https://www.rudderstack.com/blog/identity-graph/> 7- <https://about.ads.microsoft.com/en>
- 8- <https://www.shopify.com/in>
- 9- <https://www.squarespace.com>
- 10- [what-is-a-customer-data-platform-cdp](#) 11- [Google Analytics](#)

#### Meta

- 1- [crime-and-punishment-in-the-metaverse-a-primer](#)
- 2- [what-is-extended-reality-technology-a-simple-explanation-for-anyone](#) 3-  
<https://www.mdpi.com/2673-8392/2/1/31>
- 4- <https://www.happiestminds.com/blogs/the-metaverse-isnt-coming-it-is-already-here/> 5-  
<https://press.uchicago.edu/ucp/books/book/chicago/A/bo209942751.html>
- 6- <https://www.who.int/data/gho/publications/world-health-statistics>

## **Metaverse -**

The term comes from the Greek word 'meta,' which means after or beyond, combined with 'verse,' referring to the universe and used as a metaphor for the physical world. It allows users to interact through multiple senses without being limited by time or space, using their virtual representations called 'avatars.' Through these avatars, users can work, socialize, run errands, and carry out financial transactions.

### **Achieving everlasting life within the metaverse-**

Since the beginning of human existence, people have been searching for a way to achieve immortality. This desire can be seen in the pursuit of fame through creative works of art, the efforts of athletes to be remembered forever, and the construction of monuments and memorials by many rulers who wanted to leave a lasting impression for future generations. In modern times, the development of information technology, especially Web 2.0, has allowed users to interact, collaborate, connect, and share digital content. When a person passes away, they leave behind a record of their online activity known as a digital footprint. Personal and public information is stored in digital databases across the internet in the form of metadata, which together make up a person's digital legacy. This entire system contributes to the concept of "Digital Immortality." The development of artificial intelligence has enabled people to interact with the profile of a deceased user after their death. AI tools collect, analyze, and combine data available about the deceased user online to generate responses that mimic the user's behavior. Recently, Microsoft patented a chatbot that allows users to communicate with deceased individuals. When integrated with the metaverse, this technology could lead to the possibility of digital immortality. Even after a user's physical death, their AI avatar can continue to exist in the metaverse independently and carry out its functions without requiring the deceased's consent. The avatar creates responses and actions based on the user's past behavior, including body language, facial expressions, and decision-making patterns. While the idea of digital immortality in the metaverse is still being explored, it could become an exciting concept once implemented. However, it also raises a range of complex issues, including social, legal, and psychological challenges.

1 - <https://www.researchgate.net/publication/269508947> Search for Immortality in Ancient and Modern Sport

2-<https://archive.org/details/in.gov.ignca.46869/page/n39/mode/2up>

3-[https://www.researchgate.net/publication/3426898\\_Understanding\\_Web\\_20](https://www.researchgate.net/publication/3426898_Understanding_Web_20) 4-  
<https://www.ibm.com/think/topics/digital-footprint>

5- <https://pmc.ncbi.nlm.nih.gov/articles/PMC8616748/>

6 - <https://edition.cnn.com/2021/01/27/tech/microsoft-chat-bot-patent/>

[index.html#:~:text=A%20patent%20granted%20to%20Microsoft%20\(MSFT](https://www.cnn.com/2021/01/27/tech/microsoft-chat-bot-patent/index.html#:~:text=A%20patent%20granted%20to%20Microsoft%20(MSFT)

)

[%20last%20month,filing%20with%20the%20US%20Patent%20and%20Trademark%20Office.](https://www.cnn.com/2021/01/27/tech/microsoft-chat-bot-patent/index.html#:~:text=A%20patent%20granted%20to%20Microsoft%20(MSFT%20last%20month,filing%20with%20the%20US%20Patent%20and%20Trademark%20Office.)

## Social Effects-

### 1- Managing the avatar-

The concept of immortality in the metaverse brings up several complex issues, such as how independent an avatar might become after the user's death in the real world. As technology continues to develop, avatars in the metaverse can achieve a significant level of autonomy with the aid of AI tools. By analyzing metadata such as voice, facial expressions, speech patterns, preferences, and decision-making tendencies, these avatars can mimic the personality and behavior of the deceased user, enabling them to stay active in the digital space even after their physical death. This could lead to the avatar performing actions that were not originally intended. While the autonomous behavior of the avatar may offer comfort and a sense of connection for the deceased's loved ones, in keeping with the original aim of achieving immortality through the metaverse, providing such independence also imposes a responsibility on the creators and administrators of the metaverse to set clear limits on the avatar's actions.

1- <https://www.niso.org/publications/understanding-metadata-2017>

2- [you-could-become-immortal-in-the-metaverse-with-new-live-forever-mode](#)

## **2- Deviation from ethical human behavior**

There may be significant concerns about the authenticity and reliability of these interactions, especially considering the AI algorithm's ability to self-learn, which could lead the avatar to act in ways that conflict with its user's moral values. The avatar is able to absorb and adjust to new information, forming new decision-making processes through its engagement with the digital environment, which might result in behaviors the user would not endorse. Actions that violate the ethical standards of the deceased user, such as participating in illegal activities, could harm the deceased user's reputation in society. Therefore, the primary challenge for developers is to manage the avatar's autonomy and adaptability while ensuring its behavior stays within the ethical and social limits set by the deceased user, while also allowing it to respond to changes in both the real and digital worlds. The risks associated with the avatar's self-learning capabilities can be minimized by programming it to stop processing and learning new data immediately after the user's death.

## **3- The concept of life and death- The Bhagwat Geeta Says "The soul is never born, nor does it ever die."**

The Bhagavad Gita explains that all living beings go through transformation and ultimately meet death, as true happiness cannot exist without change. Just as the weather and our clothing change, the soul transitions from one body to another. Change is a fundamental aspect of life. However, in the modern world, new technologies often encourage us to hold on to the past rather than letting it go. I think this is similar to clinging to an old item and constantly looking at it, which brings pain as we remember how life used to be. Life is valuable and should be experienced in the present moment. Indian philosophy has always emphasized that we are never truly destroyed, only transformed. Real peace comes from embracing change and learning to release the past.

Now add few line

1- <https://www.radhakrishnatemple.net/blog/bhagavad-gita-quotes-on-death/>

## **Legal challenges -**

### **1- Who Owns Your Heritage?**

Now, think about this in the digital age: each social media profile is like a digital heirloom. However, unlike traditional heirlooms passed down through generations, digital profiles are jointly owned with a company. "While you're alive, you share ownership with, for example, Meta or Google," Ohman explains. "But once you're gone, they become the only owners."

In places like Europe, strict privacy laws end upon death, allowing companies to manage or take advantage of the data as they see fit.

### **2- Onus Liability-**

It becomes crucial to identify who is responsible for liability when an avatar performs an unlawful action. This leads to a questionable issue: who should be held accountable for the actions of a deceased user's avatar the platform, the avatar itself, the deceased user, family members, or close associates? Answering this question presents a challenge within the metaverse, as current legal systems are not well-suited to address the wrongdoing carried out by avatars in this digital environment.

For an action to be classified as a crime, four key elements must be present: a human action, mens rea (the intent to do wrong), actus reus (an unlawful act or omission), and some kind of harm resulting from the action. These factors are essential for establishing criminal responsibility in a legal context. However, when dealing with wrongful acts performed by avatars in the metaverse, mens rea may not be applicable, as the user is no longer alive, and avatars could exhibit such behaviors based on data from the deceased user or through interactions within the metaverse's digital environment.

At present, AI systems are still unable to differentiate between right and wrong, as demonstrated by recent cases, such as an AI robot called "Muhammad" harassing a female journalist in the UAE and a 16-year-old girl experiencing digital rape. Experts have suggested treating AI robots as legal entities and making them responsible for their actions. By the same logic, avatars could also be regarded as legal entities, thus holding them accountable for their behavior. Although the harmful actions of an avatar take place in the digital world, they can still inflict significant psychological damage on victims. Looking forward, the use of haptic devices may further complicate the

distinction between digital and physical interactions, enabling users to feel sensations like touch or groping in the metaverse, even though these are only sensory experiences and not physically real.[6] Section 75 of the Bharatiya Nyaay Sanhita, 2023 states that physical contact is not required for an act to be considered sexual harassment; however, it is still uncertain whether an act directed at a representation of the victim can constitute an offence under these circumstances.

- 1- [https://www.thehindu.com/sci-tech/technology/virtual-gang-rape-reported-in-the-metaverse-probe-underway/article67705164.ece#google\\_vignette](https://www.thehindu.com/sci-tech/technology/virtual-gang-rape-reported-in-the-metaverse-probe-underway/article67705164.ece#google_vignette)
- 2- <https://docs.manupatra.in/newslines/articles/Upload/4e5c9c80-320b-4433-9f87-f56059a5345c.pdf>
- 3- <https://www.forbes.com/sites/bernardmarr/2024/01/16/the-metaverse-and-its-dark-side-confronting-the-reality-of-virtual-rape/?sh=67dcdcf02b66>
- 4- <https://www.liebertpub.com/doi/10.1089/cyber.2023.29278.editorial>

### **3- Indian act about the data protection of the citizen-**

In practice, managing personal data after it has been sent to another country poses significant challenges. Foreign companies may not be legally required to quickly follow instructions from Indian authorities, particularly when there are no effective international enforcement mechanisms in place. Once personal data is copied, shared, or sold among different organizations, it becomes nearly impossible to completely retrieve or delete it from all systems. Additionally, the lack of a strong and unified global data protection framework limits individuals' ability to maintain true control over their information. These jurisdictional obstacles, technological constraints, and regulatory shortcomings collectively make cross-border data protection one of the most complex issues in modern data governance.

The Digital Personal Data Protection Act of 2023, together with the 2025 Rules, provides individuals with important rights, including the ability to access, correct, delete, and resolve grievances related to their data, which can be exercised through formal procedures such as submitting requests or lodging complaints with the Data Protection Board. However, these mechanisms demand a certain level of legal and digital literacy. In the metaverse and on platforms such as Facebook, this creates a significant barrier for individuals who are economically

disadvantaged or lack digital awareness, as they often do not know how to assert their rights or seek assistance when their data is collected or sold without consent. Although legal remedies exist, they are often inaccessible in practice. This problem becomes even more pronounced when avatars in the metaverse violate individuals' rights or dignity, as there is currently no clear avenue or specific system to address such complaints. The landmark judgment in Justice K.S. Puttaswamy (Retd.) v. Union of India recognized privacy as a fundamental right, yet transforming this constitutional guarantee into practical enforcement remains a significant challenge. Unsolicited emails, Custom instructions: Targeted advertisements and constant digital disturbances are already consuming valuable time and mental effort. If these problems are not resolved, they may lead to long-term digital stress for future generations, undermining both respect and trust in emerging technologies.

1- <https://www.thehindu.com/business/Industry/customers-wary-of-how-companies-use-their-personal-data-finds-survey/article24130175.ece>

2- <https://www.pib.gov.in/PressNoteDetails.aspx?NoteId=156054&ModuleId=3&reg=3&lang=2>

#### **4- Digital assets: Transfer and Succession -**

Digital data comes in various forms, including online banking accounts, cryptocurrency holdings, social media profiles, personal blogs, or digital diaries, all of which together form an individual's digital estate. However, not all digital assets we regularly engage with can be considered personal property. For example, social media accounts on platforms such as X, Facebook, or Instagram are subject to the terms of service of those platforms, which do not classify them as the user's own property. Assets that are owned by the user can be transferred through a will, or if there is no will, they are passed on to the legal heir, similar to physical possessions. Interestingly, once a user's digital avatar becomes independent after their death, it is unclear whether the avatar might inherit the user's digital assets instead of the biological heir. Another possibility is that the assets could be split between the biological heir and the avatar, depending on the user's wishes.

1- <https://www.louisianasuccessionattorney.com/blog/death-and-the-digital-estate.cfm>

Psychological Consequences-

Recent events in India highlight the serious misuse of personal data and artificial intelligence

through deepfakes for purposes such as blackmail, extortion, and the spread of fake news. In Faridabad, a 19-year-old student committed suicide after being extorted with indecent AI-generated images. In Ghaziabad, a 76-year-old man was blackmailed using a deepfake video of a retired IPS officer, which caused him significant psychological distress. These incidents demonstrate how deepfake technology is increasingly being used as a tool to produce fake nude images, fabricated videos, and misleading profiles to intimidate innocent individuals, especially women, resulting in social stigma, the breakdown of marriages, and familial rejection. In addition to personal extortion, fake news channels and digital platforms are also using manipulated content to gain attention, spread false information, and promote low-quality or fraudulent products for commercial purposes. These tactics take advantage of public trust and the slow pace of regulatory systems to generate profit. While legal solutions are available under the IT Act and cybercrime laws, victims often face challenges due to limited awareness, slow investigations, and the difficulty of tracking digital evidence. The merging of deepfake misuse, false information, and data breaches poses a significant danger to personal dignity, privacy, and societal stability in the digital era.

- 1- [https://timesofindia.indiatimes.com/city/gurgaon/blackmailed-by-ai-generated-pictures-student-dies-by-suicide-in-faridabad/articleshow/124833566.cms?utm\\_source=chatgpt.com](https://timesofindia.indiatimes.com/city/gurgaon/blackmailed-by-ai-generated-pictures-student-dies-by-suicide-in-faridabad/articleshow/124833566.cms?utm_source=chatgpt.com)
- 2- [https://economictimes.indiatimes.com/news/new-updates/man-gets-caught-in-deepfake-trap-almost-ends-life-among-first-such-cases-in-india/articleshow/105611955.cms?utm\\_source=chatgpt.com&from=mdr](https://economictimes.indiatimes.com/news/new-updates/man-gets-caught-in-deepfake-trap-almost-ends-life-among-first-such-cases-in-india/articleshow/105611955.cms?utm_source=chatgpt.com&from=mdr)
- 3- [https://indianexpress.com/article/technology/tech-news-technology/how-deepfake-tech-is-weaponised-and-how-to-fight-back-9771402/?utm\\_source=chatgpt.com](https://indianexpress.com/article/technology/tech-news-technology/how-deepfake-tech-is-weaponised-and-how-to-fight-back-9771402/?utm_source=chatgpt.com)
- 4- [https://timesofindia.indiatimes.com/city/bengaluru/love-sex-aur-dhokha-bengaluru-based-techie-strips-for-ai-girlfriend-falls-into-sextortion-racket/articleshow/126421332.cms?utm\\_source=chatgpt.com](https://timesofindia.indiatimes.com/city/bengaluru/love-sex-aur-dhokha-bengaluru-based-techie-strips-for-ai-girlfriend-falls-into-sextortion-racket/articleshow/126421332.cms?utm_source=chatgpt.com)
- 5- [https://rajatsharma.in/beware-of-fake-news-channels-deepfake-cyber-frauds/?utm\\_source=chatgpt.com](https://rajatsharma.in/beware-of-fake-news-channels-deepfake-cyber-frauds/?utm_source=chatgpt.com)
- 6- [https://www.vice.com/en/article/india-instagram-sextortion-phishing-deepfake-porn-scam/?utm\\_source=chatgpt.com](https://www.vice.com/en/article/india-instagram-sextortion-phishing-deepfake-porn-scam/?utm_source=chatgpt.com)

## Conclusion -

I would like to ask a simple question: are we truly willing to sacrifice our privacy? The obvious answer is no, because nobody wants their personal lives to become a future issue. Recently, news reports on TV and in newspapers mentioned a statement allegedly made by “Ajit Doval” regarding the use of Android devices. It was said that he avoids using Android phones because of the ongoing risk of personal data and privacy being compromised. While there may be other, supposedly more secure technologies available, what about the millions of everyday people who still use Android devices every day? A large portion of society engineers, lawyers, doctors, and others professionals rely on high-end smartphones, assuming these devices provide strong privacy protection. Companies often claim that their products are secure and respect user privacy. However, this belief is usually wrong. Even the most advanced devices continuously collect personal information through apps, permissions, sensors, and background processes, most of which users neither understand nor control.

The vulnerability becomes increasingly alarming with the rise of deepfake technology, autonomous 3D avatars, and major data breaches. Deepfakes enable identity manipulation, blackmail, harm to one's reputation, and social exclusion, while avatars may continue to represent a person even after their death. Nowadays, data theft causes more than just financial loss; it also threatens personal dignity, mental health, family life, and social standing. In conclusion, unless strong legal safeguards, effective enforcement, and widespread digital awareness are quickly implemented, the future may bring a society where privacy, identity, and truth lose their importance in the digital realm.

- 1- <https://economictimes.indiatimes.com/news/new-updates/ajit-doval-indias-james-bond-says-he-does-not-use-mobile-internet-for-day-to-day-work/articleshow/126479247.cms?from=mdr>
- 2- <https://www.mcafee.com/blogs/family-safety/digital-assets/>
- 3- <https://ari.nus.edu.sg/people/dr-connor-graham/>
- 4- <https://communication.umd.edu/directory/grant-bollmer>