Jus Corpus Law Journal

Open Access Law Journal – Copyright © 2024 – ISSN 2582-7820
Editor-in-Chief – Prof. (Dr.) Rhishikesh Dave; Publisher – Ayush Pandey

Privacy in Peril: Rise of Data Breaches in the Entertainment and Media Industries

Radhika Subhash Tapkir[a]

[a]Army Institute of Law, Mohali, India

Received 19 March 2024; *Accepted* 22 April 2024; *Published* 25 April 2024

The increased utilisation of technology and artificial intelligence in the entertainment and media industries has brought about a storm of cybersecurity issues. This paper aims to identify and analyse several common patterns and factors relating to cyber vulnerabilities faced across both industries worldwide. Furthermore, the paper sheds light on customer trust, and crisis strategies adopted for mitigating cybercrimes, financial losses, reputational damage, and other vulnerabilities. The current situation indicates a rise in data breaches, often targeting the consumer's personal data. Such blatant identity and data theft poses a grave threat to the privacy of consumers. The regulatory frameworks involving cyber and privacy provisions vary globally, providing a wider perspective into the legal consequences of such crimes. The paper discusses these regulatory provisions with the help of prominent examples of data breaches in both industries, involving major companies such as Netflix and HBO. The digital systems used in these industries have made them a lucrative target for cybercriminals, as intellectual property theft is often a collateral part of data breaches. The paper concludes with an emphasis on the importance of cyber security measures, addressing the rise of specific cyber issues, and evolving compliance landscapes to safeguard against such cyber-attacks.

Keywords: *cybersecurity, data breaches, data protection, identity theft, media industry, entertainment industry.*

INTRODUCTION

The urban societal dependence on technology and AI is proving to be a double-edged sword. The integration of technology to modernise and improve the quality of living standards in our existing societies has led to the rise of a new set of challenges. As we move to a technology-embedded future, it is essential to address these challenges and ensure the safety of individuals in this cyber age through structurally sound legal and ethical frameworks.

Producing a movie is an expensive and time-consuming affair. Most cybercriminals targeting successful entertainment companies and media houses rationalise their hacking and blackmailing actions, as an aspiration to extort financial gains. Oftentimes, the competitive nature of both industries and their players is underestimated. The massive amount of content generated each year is always stuck in a vicious cycle of getting their 'big' release, capturing geographical markets, and catching the attention of their consumer base.

Cybercriminals take advantage of weak and questionable cyber security, often found in the servers of entertainment and media companies. Stealing data from these companies, such as consumer statistics, personal data of employees, access controls to databases, movie scripts, unreleased content, or simply erasing the databases of media companies for ransom and monetary incentives, compromises the reputation of the company and the trust of the consumer.

In this paper, the effects of data breaches are discussed. A 'data breach' is defined under Article 4(12) of the General Data Protection Regulation, 2018 as 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.'[1]

CYBERSECURITY CONCERNS IN THE ENTERTAINMENT AND MEDIA INDUSTRIES

Cybercrimes have evolved with the evolution of technology itself. Cybersecurity concerns in the entertainment and media industries have seen exponential growth in the past decade. Media and entertainment companies are not appropriately safeguarded against the cyber risks of the

[1] General Data Protection Regulation 2018, art 4(12)

technologically advanced world. Cybercriminals are exploiting this loophole to extort money, steal data, and sell it to the highest bidder in the market.

Cybersecurity threats could be perpetuated by a variety of sources. But in the case of entertainment and media industries, the most common attackers are malicious individual hackers, cyber-crime organisations, or an insider or groups of insiders, responsible for financial and economic theft via extortion through phishing mail, data breaches, stealing personal data, and using ransomware or spyware.

Cyber-attacks in such industries can be classified as 'malware attacks', 'distributed denial of service attacks', 'man in the middle attack' and 'social engineering attacks.'[2] The cases discussed in this paper are mostly seen as victims of ransomware, spyware, and phishing.

SUSCEPTIBILITY TO CYBER RISKS BY THE ENTERTAINMENT AND MEDIA INDUSTRY

As movies, TV series, games, and news outlets adopt digital personalities for better reach and expansion of audience, the cybercriminals view it as a new source of monetary extortion as well as gaining access to oftentimes valuable resources such as the scripts of movies, books, etc. and pirating them to open access websites. The following are the risks associated with the industries:

Sensitive Information Leak & Piracy:

Earlier, piracy was conducted through physical CDs and DVDs, but the easy access to inexpensive internet along with rapid technological advancement has led consumers to download films, music, games, software, etc. from online piracy sources like Torrent.

The music industry is particularly affected by piracy, with a record 15 billion visits to music piracy sites in 2022 alone, according to MUSO (a UK technology company). MUSO also detected 40% of illegal downloads coming from the US, it included illegal downloads of David Bowie's

[2] 'Cybersecurity Threats' (*Imperva*) <https://www.imperva.com/learn/application-security/cyber-security-threats/> accessed on 10 March 2024

music (950,000 downloads), Bruce Springsteen's catalogue (780,000 downloads), Bob Dylan's release (750,000 downloads), and Justin Bieber's entire discography (more than 1 million downloads).[3]

Napster in 1999 was a topic of debate.[4] It was viewed with two different opinions. One set of people arguing against it due to the accessibility of downloading unlicensed MP3s grew exponentially. Another set viewed the service as a preview opportunity as a 'try before you buy'.[5]

In 2017, full episodes of the famous Netflix show 'Orange Is the New Black' were dumped by the hacker group known as 'The Dark Overlord'. This was allegedly done due to Netflix's refusal to pay the demanded ransom.[6] Additionally, The Dark Overlord had also threatened to release episodes of other Netflix titles (approximately 37 titles/shows) such as AboveSuspicion (TV series), Handsome (film), Mega Park (TV series), The Arrangement (TV series) and many others. This group has previously been associated with multiple cyber-attacks and data leaks related to the healthcare and medical industries.

With an increase in the OTT culture in India, the consumption of movies and web series on illegal forums has grown exponentially. It is estimated that 25-50% of the revenue of OTT platforms is affected by piracy, as per Gourav Rakshit (COO, Viacom18 Digital Ventures).[7] According to the Managing Director of Aiplex (an anti-piracy agency based in Bengaluru), 'a

[3] Elias Leight, 'Music Piracy Is Rising — And the U.S. Is a Trouble Spot' (*Billboard*, 03 September 2023) <www.billboard.com/pro/music-piracy-2022-stream-ripping/> accessed 07 February 2024

[4] Eamonn Forde, 'Oversharing: how Napster nearly killed the music industry' *The Guardian* (31 May 2019) <www.theguardian.com/music/2019/may/31/napster-twenty-years-music-revolution> accessed 07 February 2024

[5] Adam Sherwin, 'Fans who download music 'buy more CDs' *The Times & The Sunday Times* (09 July 2003) <www.thetimes.co.uk/article/fans-who-download-music-buy-more-cds-q8kg9n9g7lg> accessed 07 February 2024

[6] Tom Huddleston Jr, 'Hackers Leaked 'Orange Is the New Black' Despite Receiving $50,000 Ransom' (*FORTUNE*, 22 June 2017) <https://fortune.com/2017/06/21/hackers-leaked-orange-is-the-new-black-ransom/> accessed 01 February 2024

[7] Nisha Qureshi, 'As OTT platforms lose up to 50% subscription revenue to piracy, CII on war mode to tackle problem: Best Media Info' (*Best Media Info*, 12 February 2021) <https://bestmediainfo.com/2021/02/as-ott-platforms-lose-up-to-50-subscription-revenue-to-piracy-cii-on-war-mode-to-tackle-problem> accessed 11 January 2024

report by Digital TV Research in 2021, the loss of revenue for OTT players on account of piracy in India is expected to hit $3.08 billion by 2022, while the cost of global online streaming piracy will reach $52 billion by 2022.'[8]

Simply put, content is the most valuable possession in the media and entertainment industries. It is their job to make sure it is well-protected and confidentiality is maintained in regards to their matter.

Insider Threats:

In every movie, TV show, or media coverage, there are various internal and external stakeholders involved. Insider threats are defined by IBM as 'cybersecurity threats that originate within authorised users - employees, contractors, and business partners - who intentionally or accidentally misuse their legitimate access, or have their accounts hijacked by cybercriminals.'[9] Sometimes the competitors of an organisation might bribe or coerce an employee to divulge confidential information or trade secrets to them. Sometimes the team handling the intellectual property of a film might be responsible for its theft or leak on the dark web.

Such individuals, having access to the personal data of other individuals, sensitive information, financial records or transactions, encryption keys to databases, etc., and the availability of resources within the organisation, can easily steal the information and sell it to their competitors for monetary gains.

Insider threats could be a result of three types, namely, malicious insiders, negligent insiders, and compromised insiders.[10]

[8] Mohua Das, 'Torrents to Telegram, piracy makes a comeback in OTT era' *The Times of India* (18 August 2022) <https://timesofindia.indiatimes.com/times-special/torrents-to-telegram-piracy-makes-a-comeback-in-ott-era/articleshow/93645484.cms?from=mdr> accessed 06 February 2024
[9] 'What are insider threats?' (*IBM*) <www.ibm.com/topics/insider-threats> accessed 6 February 2024
[10] 'Three Types of Insider Threats (and How to Stop Them)' (*Proof Point,* 17 February 2021) <https://www.proofpoint.com/us/blog/insider-threat-management/three-types-insider-threats-and-how-stop-them> accessed 18 February 2024

Here are some cases of such incidents:

1. A former Twitter employee has been sentenced to 30 years of imprisonment along with a fine of $250,000 for various counts of offences, including fraud, international money laundering, conspiracy, and user information theft, in 2022. Ahmad Abouammo (44 years old), while employed at Twitter, furnished private information about Twitter users to the officials of Saudi Arabia and the Saudi Royal Family. Abouamma was employed by Twitter to protect Twitter user information. Multiple monetary transactions were found to have been made to Abouammo by the Royal family for the information.[11]

2. In 2023, two former Tesla employees orchestrated a data leak and disclosed the personal information of 75,735 people as per Tesla's data breach notification.[12] The leaked data contained the names, addresses, phone numbers and email addresses of former and current employees. Tesla filed a lawsuit to obtain the digital devices (believed to contain stolen data) of those two former employees.[13]

3. A former Google employee was sentenced to prison for 18 months and fined $95,000 for trade secret theft and paid $756,499.22 in restitution to Waymo LLC (Google's self-driving program now). Anthony Scott Levandowski (40 years old), while leaving Google in 2016, downloaded files relating to Google's 'Project Chauffeur' on his laptop. He admitted during his trial that the files were downloaded with 'an intent to benefit himself and Uber Technologies, Inc.' He later

[11] 'Former Twitter Employee Found Guilty of Acting as an Agent of a Foreign Government and Unlawfully Sharing Twitter User Information' (*Department of Justice*, 10 August 2022) <https://www.justice.gov/opa/pr/former-twitter-employee-found-guilty-acting-agent-foreign-government-and-unlawfully-sharing> accessed 18 February 2024

[12] 'Data Breach Notification' (*Office of the Maine Attorney General*) <https://apps.web.maine.gov/online/aeviewer/ME/40/014ae6db-4cb7-464b-b827-5d73f0bbc911.shtml> accessed 28 January 2024

[13] Derek B. Johnson, 'Tesla says former employees leaked thousands of personal records to German news outlet' *SC Media* (21 August 2023) <https://www.scmagazine.com/news/tesla-says-former-employees-leaked-thousands-of-personal-records-to-german-news-outlet> accessed 28 January 2024

also admitted to the court that he was aware of the sensitive and confidential nature of the information.[14]

Unlike the above malicious or negligent insiders, in the scenario of a compromised insider, it usually occurs in the form of credential or login information theft. The employee's login information and credentials become compromised, leading to easy access to hackers or cybercriminals. Such compromised insiders have cost their organisation more than $4.6 million in 2021-2022.[15]

INTERNAL IMPACT OF DATA BREACHES IN THE ENTERTAINMENT AND MEDIA INDUSTRIES

The consequences of data breaches have far-reaching implications, especially for the intellectual property assets of these companies. It is every filmmaker's nightmare and every hacker's dream to gain access to copyrighted assets of any content. It can be turned into blackmail material, can be used to extort handsome ransoms, or pirated to and from illegal websites and dealers.

Technological advancement has turned into a double-edged sword for the media industry. On one hand, there is a heavy reliance on digital infrastructure for editing, storing, and producing content and data. However, the cyber attackers are taking advantage of weak digital infrastructure, a lack of physical access, or to purely spite a media/entertainment company[16] and have started popping up like poisonous mushrooms everywhere. Sony Pictures had to dole out $8 million in fines for employees' data being hacked in 2014-15.[17] The data breach was led by a group called the Guardians of Peace. A movie named 'The Interview', an American-North

---

[14] 'Former Uber Executive Sentenced To 18 Months In Jail For Trade Secret Theft From Google' (*Department of Justice | Homepage | United States Department of Justice*, 4 August 2020) <https://www.justice.gov/usao-ndca/pr/former-uber-executive-sentenced-18-months-jail-trade-secret-theft-google> accessed on 28 January 2024

[15] Brian Reed, 'Insider Threats (Still) On the Rise - Facts & Data | Proofpoint US' (Proofpoint, 25 January 2022) <https://www.proofpoint.com/us/blog/insider-threat-management/insider-threats-are-still-rise-2022-ponemon-report> accessed on 28 January 2024

[16] Ted Johnson, 'Sony Hack Attack Opens Minefield of Legal Questions That Has Hollywood Worried' (*Variety*, 14 April 2015) <https://variety.com/2015/biz/news/sony-hack-attack-opens-minefield-of-legal-questions-that-has-hollywood-worried-1201471664/> accessed 18 January 2024

[17] 'Sony pays up to $8m over employees' hacked data' *BBC News* (21 October 2015) <www.bbc.com/news/business-34589710> accessed 18 January 2024

Korean comedy was blamed as the reason for hackers' releasing datasets of personal information in an attempt to derail its release. Thousands of Disney+ accounts were hacked and put on sale on various platforms.[18] This incident took place in the video-streaming services' first week itself, acting as an omen for worse cyber breaches to come.

Here are the following consequences of cyber-attacks and data breaches that can affect such industries and businesses:

Loss of Intellectual Property: Lewis Lee (Chief Executive Officer, Aon Intellectual Property Solutions)[19] stated, 'Across industries, intangible assets are becoming primary sources of value. Over the past decade, intangible assets have begun to overtake tangible assets. …Copyrights, patents, formulae, and source code have overtaken [physical] property or equipment as some of the most valuable items on a balance sheet.'[20]

The digitalisation has made the theft of intellectual property a complex task. Intellectual property in its various forms remains under constant threat, such as - copyrights, trademarks, patents, trade secrets, and designs. It should be recognised that any type of intellectual property in such successful industries has value even in its nascent developmental stages, and hence possesses enough value to lure in competitors or threats. Therefore, an IP in digital format should be protected against any potential cyber risk or adversaries in all stages of the life cycle.[21]

[18] Catalin Cimpanu, 'Thousands of hacked Disney+ accounts are already for sale on hacking forums' (*ZDNET*, 16 November 2019) <www.zdnet.com/article/thousands-of-hacked-disney-accounts-are-already-for-sale-on-hacking-forums/> accessed 25 January 2024

[19] 'Insights' (*AON*) <https://www.aon.com/en/insights?searchStudioQuery=&isGrid=false&facets=&orderBy=&start=0&facetTopic=1&facetFunction=1&facetContent%20Type=1&facetLocation=1&facetIndustry=1> accessed 14 January 2024

[20] 'Cyber Criminals on the Hunt for IP Riches' (*AON*) <https://www.aon.com/unitedkingdom/insights/cyber-criminals-on-the-hunt-for-ip-riches.jsp> accessed 14 January 2024

[21] John Patrick Gelinne et al., 'The hidden costs of an IP breach: Cyber theft and the loss of intellectual property' (*Deloitte Insights*, 26 July 2016) <https://www2.deloitte.com/us/en/insights/deloitte-review/issue-19/loss-of-intellectual-property-ip-breach.html> accessed 12 February 2024

Financial Loss and Insurance Liability: According to Ponemon's Data Breach Impact Study[22], a loss of 5 percent of any organisation's customers could lead to an average revenue loss of nearly $ 4 million.[23]

One of the biggest factors that has contributed towards financial loss is piracy. There are only two commendable aspects of piracy, i.e., it helps generate the popularity of the film or TV series and makes it accessible to the masses who cannot access it through authorised or paid channels.

It is a prevalent global issue and affects the local as well as the international markets of film distribution. The impact of financial losses can certainly affect future projects of the said film studio or actors.

Indian cinema has felt the brunt of piracy. Every year, the Indian film industry loses around Rs. 2000 crore to piracy.[24] One of the biggest examples of piracy victims is Baahubali. It was the most expensive movie with a multi-million-dollar budget, yet it suffered a financial loss of approximately Rs. 1,064 crores due to piracy. This damaged the business of the film, negatively affecting its profits. Such financial losses affect the royalties, payments, and benefits meant for the workers, actors, producers, directors, etc.

Fox Studios released an apt statement when a copy of their movie titled 'Wolverine' was pirated before its official release in theatres, stating that, 'the theft of the movie undermines the enormous efforts of the filmmakers and actors and, above all, hurts fans of the film.'[25]

---

[22] 'Home | Ponemon Institute' (*Ponemon Institute*) <https://www.ponemon.org/> accessed on 12 February 2024
[23] 'Loss of Trust: A Cybersecurity Attack's Invisible Consequence' (*SIA Innovations*) <https://www.siainnovations.com/blog/loss-of-trust-a-cybersecurity-attacks-invisible-consequence/> accessed 12 February 2024
[24] Ganesh Aaglave, 'Thugs of Bollywood! Raees, Sultan, Dilwale are the most PIRATED films ever | Bollywood Life' (*Bollywood Life*, 3 February 2018) <https://www.bollywoodlife.com/news-gossip/thugs-of-bollywood-raees-sultan-dilwale-are-the-most-pirated-films-ever-1150882/> accessed 12 February 2024
[25] Daniel Nasaw, 'Upcoming X-Men movie leaked online ahead of release' *The Guardian* (Washington, 2 April 2009) <https://www.theguardian.com/world/2009/apr/02/wolverine-xmen-leak-online-piracy> accessed 29 January 2024

The data breach negatively affects the stock prices of the companies.[26] Such a cyber incident might reflect on the company's commitment to privacy and cyber security, following which the investors might lose confidence in the company's ability to manage and avoid risks or threats.

Damage to Reputation and Breach of Customer Trust: Every corporation and company views 'reputation' as a strategic intangible asset because it contributes to their competitive edge in the market. Therefore, reputational damage of any sort could potentially impact the company's image, and its ability to secure a future customer base and financial investments. A data breach in any sector would garner negative media publicity, damaging the reputation of the business in the eyes of the general public. It creates an atmosphere of negativity and dissent towards the company, resulting in difficulty in attracting new customers and expanding of business in general.

Customers value transparency from organisations that handle their data. In a world surrounded by digital appliances 24/7, customer data has become a valued gem. In case of a data breach or other cyber-attack, the customers expect the company or organisation to explain the how and why of the issue in clear words while also reassuring them that appropriate actionable solutions have been implemented to prevent the problem from spreading further and recurring.

Targeted cyber-attacks often expose the data of innocent customers online or sell it to nefarious parties for monetary gain. Such a loss of personal data could lead to a multitude of other cybercrimes, such as identity theft and credit card credential theft.[27] In July 2021, almost 1500 small businesses experienced a ransomware attack.[28] The attack was a result of a previously

[26] Kevin M. Gatzlaff and Kathleen A. McCullough, 'The Effect of Data Breaches on Shareholder Wealth' (2010) 13(1) Risk Management and Insurance Review <https://doi.org/10.1111/j.1540-6296.2010.01178.x> accessed 02 March 2024

[27] Loss of Trust: A Cybersecurity Attack's Invisible Consequence - SIA Innovations (n 23)

[28] Liam Tung, 'Kaseya ransomware attack: 1,500 companies affected, company confirms' (*ZDNET*, 6 July 2021) <https://www.zdnet.com/article/kaseya-ransomware-attack-1500-companies-affected-company-confirms/> accessed 22 February 2024

undetected fault in the Kaseya software, commonly used by these businesses. The customers of these companies were informed about the attack through email and online notices.[29]

A GLOBAL PERSPECTIVE: REGULATORY FRAMEWORKS & LEGAL CONSEQUENCES

As of March 2023, more than 162 countries had data privacy legislation in place, with other countries having either draft privacy legislation or no privacy legislation at all.[30] Let's take a look at data privacy provisions along with examples through the lens of different regulatory frameworks across the globe:

Personal Data and its Processing: In India, issues regarding sensitive and personal data are addressed under the Digital Personal Data Protection Act, 2023. Entertainment industries, especially OTT platforms, often collect the personal data of their consumers for subscriptions to their streaming services, and therefore it can be said that Chapter II of the Act, 2023, applies to both the data controller (OTT platform) and data principal (consumer) in such cases. In 2022-23, the Ministry of Electronics and Information Technology (Meity) issued several advisories to platforms like Netflix and Hotstar, underscoring concerns over data privacy non-compliance, particularly regarding data localization and consent mechanisms.[31]

Cross-Border Transfer of Personal Information: A cross-border transfer of personal information can be understood as the transfer of personal data from one company or jurisdiction to another company or jurisdiction. We can understand this provision concerning Article 22[32] of South Korea's Personal Information Protection Act. South Korea takes the privacy of their citizens extremely seriously, by imposing strict restrictions on the transfer of personal data of Korean individuals outside of South Korea, requiring additional security measures and prior

[29] Charlie Osborne, 'Updated Kaseya ransomware attack FAQ: What we know now' (*ZDNET*, 23 July 2021) <https://www.zdnet.com/article/updated-kaseya-ransomware-attack-faq-what-we-know-now/> accessed 22 February 2024

[30] Graham Greenleaf, 'Global Data Privacy Laws 2023: 162 National Laws and 20 Bills' (2023) UNSW Law Research Paper No. 23-48 <https://papers.ssrn.com/sol3/papers.cfm?abstract_id=4426146> accessed 22 February 2024

[31] 'Meity Draft Amendment to IT. (Intermediate Guidelines and Digital Media Ethics Rules) Rules 2021' (*Tsaaro Consulting*, 11 July 2022) <https://tsaaro.com/blogs/meity-draft-amendment-to-it-intermediary-guidelines-and-digital-media-ethics-rules-rules-2021/> accessed 28 February 2024

[32] Personal Information Protection Act 2011, art 22

approvals from the relevant authorities. KakaoTalk, a popular messaging app, has been embroiled in privacy breaches and lawsuits for a very long time.[33] Netflix was fined by the Personal Information Protection Commission (PIPC) of South Korea for collecting personal information of Korean citizens without prior informed consent.[34] Netflix was also penalised for lack of transparency in the instance of not disclosing cross-border data transfers.

Another example of the violation of handling personal data in instances of cross-border transfer is the penalty imposed by Ireland's Data Protection Commission on Meta in 2023. The fine was one of the highest ever recorded in history, at a record €1.2 billion, in GDPR penalties.[35] The penalty was a result of Meta transferring data collected through Facebook from users in the European Union to the United States. This was found to be in clear violation of Article 46(1)[36] of the EU GDPR as well as the landmark judgement of the *Data Protection Commissioner v Facebook Ireland Limited and Maximillian Schrems (Schrems II)*, delivered by the European Court of Justice.[37]

Processing of Sensitive Information: Sensitive information or data seeks a higher level of protection, as such data 'includes genetic, biometric, and health data, as well as personal data revealing racial and ethnic, political opinions, religious or ideological convictions, or trade union membership' as per Article 4 of the General Data Protection Regulation 2018. Additionally, Article 9(1) of the General Data Protection Regulation 2018, prohibits the processing of such sensitive data.[38] When seen concerning the entertainment and media industries, such data can be used for the application of special effects in TV series or movies, for authentication purposes in film studios. Therefore, additional safeguards for such data and the explicit consent of the

[33] Dain Oh, 'Most popular messaging app in Korea faces controversy over security' (*The Readable*, 14 March 2023) <https://thereadable.co/most-popular-messaging-app-in-korea-faces-controversy-over-security/> accessed 28 February 2024

[34] Adv. Haim Ravia and Adv. Dotan Hammer, 'South Korea: Facebook and Netflix Fined for Privacy Infringements' (*Law.Co.Il*, 26 August 2021) <https://www.law.co.il/en/news/2021/08/26/south-korea-fines-facebook-and-netflix-privacy-infringements/> accessed 28 February 2024

[35] 'Irish Data Protection Commissioner imposes a 1.2 billion fine on Meta Ireland' (*BDO United Kingdom*, 24 October 2023) <https://www.bdo.co.uk/en-gb/insights/advisory/risk-and-advisory-services/irish-data-protection-commissioner-imposes-a-1-2-billion-fine-on-meta-ireland> accessed 01 March 2024

[36] General Data Protection Regulation 2018, art 46(1)

[37] Nikhil Girdhar, 'Learning from the Fallout: A Massive $1.3 Billion Fine for Violating EU's Cross Border Data Transfer Regulation' (*Securiti*, 06 June 2023) <https://securiti.ai/blog/1-3-billion-fine-for-violating-eu-cross-border-data-transfer/> accessed 29 February 2024

[38] General Data Protection Regulations 2018, art 9(1)

individuals for processing such sensitive data should be mandatorily implemented. In 2022, TikTok contravened the provision of Article 9 of the General Data Protection Regulation 2018, by unlawfully collecting and retaining biometric data, specifically 'facial features' of minors. The Dutch Data Protection Authority imposed a penalty of €750,000 for the same.[39]

Data Security and Transparency: It is assumed to be a common practice and belief that a company handling financial information such as credit card details, bank information, payment methods, etc. would take appropriate measures to ensure data security. In one instance, the Australian Information Commissioner issued a privacy complaint against Optus, a telecommunications company. In 2022, it was impacted by a data breach affecting millions of customers.[40] The Australian Privacy Principles[41] (APPs) and Australia's Privacy Amendment (Enhancing Privacy Protection) Act 2012 emphasise valuing data security. Entertainment and media companies handling personal data, especially user preferences, financial data, and bank information, are mandatorily obligated to take appropriate safety measures.

Data Localization: 'Data Localisation' does not have a set definition. Many scholars and privacy legislation have tried to define it according to their perspective or national and commercial requirements. It has been defined as 'a mandatory legal or administrative requirement directly or indirectly stipulating that data be stored or processed, exclusively or non-exclusively, within a specified jurisdiction.'[42]

In 2022, Russia fined Pinterest, Twitch and Airbnb for various privacy violations. Notably, Twitch, a streaming platform, was found guilty by the Tagansky District Court (Russia) for not complying with the data localisation principle and was penalised with a fine payable of 2 million

[39] 'Dutch DPA: TikTok fined for violating children's privacy' *EDPB* (Netherlands, 22 July 2021) <https://www.edpb.europa.eu/news/national-news/2021/dutch-dpa-tiktok-fined-violating-childrens-privacy_en> accessed 20 February 2024

[40] Tiffanie Turnbull, 'Optus: How a massive data breach has exposed Australia' *BBC News* (Sydney, 29 September 2022) <https://www.bbc.com/news/world-australia-63056838> accessed 20 February 2024

[41] Privacy Amendment (Enhancing Privacy Protection) Act 2012, sch 1

[42] Dan Svantesson, 'Data Localisation Trends and Challenges' (2020) OECD Digital Economy Papers No 301, 2020 <https://doi.org/10.1787/7fbaed62-en> accessed 03 March 2024

roubles.[43] Another penalty of 13 million roubles ($135,000) was dealt out to Twitch in 2023 by the Russian Courts for 'repeated failure' to comply with localising data as per the privacy legislation of Russia.[44]

There is a mutual understanding among the customers and the company, that all necessary legal compliances on the organisation's side have been taken care of. It is presumed by the user that personal data and financial data are protected by the organisation. A data breach can occur either intentionally or unintentionally, and in such scenarios, the company or the individuals should be able to take legal action, file suit, and later claim compensation for their damage.

LEGAL CONSEQUENCES OF DATA BREACHES IN THE ENTERTAINMENT AND MEDIA INDUSTRIES

The legal landscape is complex and tricky to navigate because the regulations of various countries dictate data handling and privacy practices. To understand the application of various data protection laws, it should be strongly acknowledged that the entertainment and media industries operate across borders, making compliance a multi-jurisdictional challenge.

Beyond the immediate financial and reputational damage, data breaches in these industries can trigger a complex web of legal liabilities. Firstly, in civil lawsuits, the affected individuals can sue companies for negligence in protecting their data, leading to financial compensation for damages like emotional stress, identity theft, or financial losses. In 2012, the then FBI Director Robert Mueller addressed the rise of cybercrimes and hackers into organized crime in a speech at the Cyber Security Conference held in San Francisco.[45] He emphasised the escalating costs of

[43] 'Russia fines Twitch, Pinterest and Airbnb and others for alleged data storage violation' *The Economic Times* (28 June 2022) <https://m.economictimes.com/tech/technology/russia-fines-foreign-firms-for-alleged-data-storage-violations/articleshow/92520168.cms> accessed 03 March 2024

[44] 'Russian Courts fines Tinder, Twitch for refusing to localise data' *CNBC TV18* (04 September 2023) <https://www.google.com/amp/s/www.cnbctv18.com/technology/russian-court-fines-tinder-twitch-for-refusing-to-localise-data-17714111.htm/amp> accessed 03 March 2024

[45] 'Robert Mueller, RSA Cyber Security Conference Address' (*American Rhetoric*, 01 March 2012) <https://www.americanrhetoric.com/speeches/robertmuellerrsacyberconference2012.htm> accessed 21 March 2024

settling data breaches and the resultant lawsuits filed by the affected parties.[46] An average settlement amount for data breach class-action lawsuits in the USA can run into hundreds of millions. According to a report published by IBM in 2023, 'the global average cost of a data breach in 2023 was USD 4.45 million, a 15% increase over 3 years.'[47]

Secondly, data breaches may violate contractual obligations with business partners, vendors, or clients, leading to potential lawsuits. Furthermore, in severe cases, individuals involved in a data breach might face criminal charges for unauthorised access, theft and fraud. Thirdly, in case of a data breach that violates data privacy regulations, it can result in hefty fines from the governing regulatory body. For example, the GDPR imposes penalties of up to €20 million or 4% of the global annual turnover of the organisation, whichever is higher. One such case was of Marriott International, where the hotel was fined £99 million by the ICO for a data breach affecting 339

million guest records. The fine amount was later reduced to £18.4 million.[48] Marriott International has been faced with data breach issues in 2014[49], 2015, 2020 and 2022 as well.[50]

PROMINENT DATA BREACHES

Data breaches have been a commonplace occurrence in different industries across the world. Yet, the increasing awareness regarding one's privacy rights and advancements in technology-related crimes have changed the landscape of data breaches. Article 4(12) of the General Data

[46] Fredric D. Bellamy, 'Data Breach Class Action Litigation and the Changing Legal Landscape' *Reuters* (27 June 2022) <https://www.reuters.com/legal/legalindustry/data-breach-class-action-litigation-changing-legal-landscape-2022-06-27/> accessed 21 March 2024

[47] 'Cost of a Data Breach Report 2023' (*IBM*) <https://www.ibm.com/reports/data-breach#:~:text=The%20global%20average%20cost%20of,15%25%20increase%20over%203%20years.> accessed 21 March 2024

[48] 'Penalty Notice Marriott International Inc.' (*Information Commissioner's Office*, 30 October 2020) <https://ico.org.uk/media/action-weve-taken/mpns/2618524/marriott-international-inc-mpn-20201030.pdf> accessed 03 March 2024

[49] 'Hotel chain discovers breach of customer database following acquisition of a competitor' (*Office of the Privacy Commissioner of Canada*, 15 July 2022) <https://www.priv.gc.ca/en/opc-actions-and-decisions/investigations/investigations-into-businesses/2022/pipeda-2022-005/> accessed 03 March 2024

[50] David Sehyeon Baek, 'Marriott Data Breach Analysis: 2018, 2020, and 2022' (*LinkedIn*, 18 August 2023) <https://www.linkedin.com/pulse/marriott-data-breach-analysis-2018-2020-2022-david-sehyeon-baek-/> accessed 03 March 2024

Protection Regulation (GDPR) of 2018, states that 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed',[51] would refer to as a 'personal data breach'.

1. Cases of Data Breaches in the Entertainment and Media Industries

The entertainment industry witnessed a major shift during the COVID-19 pandemic. There was a surge in online streaming services and platforms, and an exponential rise was seen in the consumption patterns of media in digital formats.

Here are some notable and prominent incidents of cyber-attacks and data breaches that have affected the entertainment, media, and online gaming industries:

CD Projekt Red (2021): CD Projekt Red is a Polish video game maker, known for their massive hits such as 'The Witcher' and 'Cyberpunk 2077'. On February 9, 2021, they were victims of a ransomware attack. This came to light through a Twitter statement by the Polish developer.[52] The unknown hackers stole data, including the source codes of Cyberpunk 2077, The Witcher 3, and other items, from their internal servers.

There was a message left on the servers by the hackers. The hackers had put in a demand for a ransom to be paid within 48 hours, but the company refused to bow down to these demands. It was found by the cyber intelligence agencies a couple of days later, that those source codes had been sold.[53] The hackers had left a note to CD Projekt claiming to have 'dumped' all their documents on the internet related to accounting, administration, legal, HR, and investor relations, etc.

Ashley Madison (2015): Ashley Madison was a popular Canadian dating service site launched in 2002. It was specifically marketed to married people seeking an extra-marital affair. The

[51] General Data Protection Regulation 2018, art 4(12)
[52] Cristina Criddle, 'Cyberpunk 2077 makers CD Projekt hit by ransomware hack' *BBC* (09 February 2021) <https://www.bbc.com/news/technology-55994787> accessed 05 March 2024
[53] 'Security Breach Update' (*CD PROJEKT*, 10 June 2021) <https://www.cdprojekt.com/en/media/news/security-breach-update/> accessed 05 March 2024

dating service even encouraged cheating on your spouse, as reflected in their tagline, 'Life is short, have an affair'.[54]

On July 19, 2015, a hacker group known as 'The Impact Team' attacked Ashley Madison's servers.[55] They threatened to leak users' personal data along with sensitive data of the company if its parent company, 'Avid Life Media' did not shut down the said dating platform and its sister website, i.e., 'Established Men'. On July 20, 2015, Ashley Madison addressed the data breach in a Twitter (now known as 'X') post.

On July 21, 2015, more than 2500 customer records were released by 'The Impact Team'. Additionally, more than 60 gigabytes worth of information was leaked on August 18, 2015, in the form of a compressed Torrent file. The link to the torrent file was also posted on the dark web.

Avid Life Media in 2017 agreed to settle two lawsuits with a consequent amount of more than $11.2 million arising from the data breaches.[56] The data breach revealed multiple fallacies in user privacy and data security measures.[57] The regulatory compliance was almost non-existent. **Here are a few examples of the same -**

- The dating website required no email verification for the creation of an account to avail of their service.
- There were multiple fake accounts, either created by the person or by somebody else impersonating them. This sheds light on multi-layered identity thefts on the site.
- To 'delete' an account permanently, a monetary payment was required. The monetary payment ensured the removal of the account from their website, as well as the claimed

[54] The Canadian Press, 'Ashley Madison dating website drops tagline 'Life is Short, Have an Affair!' (*Toronto Star*, 12 July 2016) <https://www.thestar.com/business/ashley-madison-dating-website-drops-tagline-life-is-short-have-an-affair/article_6ce34f4c-365e-58e4-b88d-090367767314.html> accessed 05 March 2024

[55] Cassandra Cross et al., 'Media discourses surrounding 'non-ideal' victims: The case of the Ashley Madison data breach' (2018) 25(1) International Review of Victimology <https://doi.org/10.1177/0269758017752410 > accessed 05 March 2024

[56] Jonathan Stempel, 'Ashley Madison's parent in $11.2 million settlement over data breach' *Reuters* (15 July 2017) <https://www.reuters.com/article/idUSKBN19Z2F3/> accessed 05 March 2024

[57] Stacy Blasiola et al., 'The Rules of Engagement: Managing Boundaries, Managing Identities' (2016) AoIR <https://spir.aoir.org/ojs/index.php/spir/article/view/9057> accessed 05 March 2024

deletion of complete personal information. However, during the investigation, it was found that the information was never deleted permanently, especially the credit card information of the users.

The data not only highlighted the lack of privacy and regulatory compliance deficiencies on behalf of Avid Life Media but also led to the exposure of several sexual predators and paedophiles using the website services with heinous intentions.

Start.ru (2022): In 2022, the Russian OTT platform, Start.ru, suffered a data breach. The initial report was recorded on August 28, 2022, when a file containing the data of 44 million members was found to be circulating on the social network. The breach affected 7.5 million consumers.[58] The stolen database contained email addresses, usernames, and phone numbers. But later, it was found that the financial information and bank information of the subscribers were untouched.

Zee5 (2021): Data from over 9 million users of Zee5, a leading OTT platform, was leaked by a hacker in 2021.[59] This data breach was discovered by an independent security researcher named Rajesh, who later tweeted about the same on Twitter (now 'X'). Initially, the platform denied any claims of being hacked and assured the users about their strict cyber security.[60] It was later found that the data of the users was being sold on the dark web.

It has been speculated that Zee5 has suffered from multiple data breaches in the past. Approximately 1023 premium accounts were compromised in May 2020. Similarly, there was a data breach in June 2020; it resulted in the loss of 150 GB of user data. It was observed that in all three incidents of data breaches, Zee5 had not notified the users about the same. This move was condemned and criticised due to its callous nature towards user privacy and their personal data (especially sensitive and financial data).

---

[58] Bill Toulas 'Russian streaming platform confirms data breach affecting 7.5M users' *(Bleeping Computers*, 30 August 2022) <https://www.bleepingcomputer.com/news/security/russian-streaming-platform-confirms-data-breach-affecting-75m-users/> accessed 06 March 2024

[59] Samarpita Banerjee, 'Zee5 denies recent data breach claims' *Business Insider India* (05 March 2021) <https://www.businessinsider.in/advertising/ad-tech/news/zee5-denies-recent-data-breach-claims/articleshow/81344102.cms#google_vignette> accessed 08 March 2024

[60] *Ibid*

HBO (2017): In 2017, HBO suffered a cyber-attack by an Iranian hacker called Behzad Mesri[61], who goes by the alias 'Skote Vahshat'. It is estimated that in July 2017 the accused stole unreleased TV series episodes, and the script of an unreleased Game of Thrones episode, was yet to be released.

The complete data breach was 1.5 terabytes and included documents relating to the finances of the channel, personal contacts of crew and cast members, social media credentials, and email addresses of employees.[62] Mesri tried to extort $6 million (in Bitcoin)[63] from HBO in July 2017 as ransom.

Funke Media Group (2020): Funke Media Group, a leading German newspaper and publisher, fell victim to a ransomware attack[64] in December 2020. The media group is responsible for publishing multiple regional titles such as Berliner Morgenpost and Westdeutsche Allgemeine Zeitung (WAZ). It resulted in a standstill in publishing processes at their printing houses, causing them to halt production of their daily newspaper and digital print editions.

The hackers had used ransomware disguised as phishing mail. Successfully corrupting and encrypting more than 6,000 laptops and systems within the media group had been affected. According to the editor-in-chief of WAZ, the data in their IT system was deemed to be 'unusable for now.'[65] A large-scale effort was put in to clean, re-install, and check all the laptops and systems affected by the breach.

The hacker group later demanded a ransom to be paid by the media group in the form of Bitcoin.

---

[61] 'Acting Manhattan U.S. Attorney Announces For Conducting Cyber Attack And $6 Million Extortion Scheme Against HBO' (*USAO-SDNY*, 21 November 2017) <https://www.justice.gov/usao-sdny/pr/acting-manhattan-us-attorney-announces-charges-against-iranian-national-conducting> accessed 06 March 2024

[62] Daniel Victor and Sheera Frenkel, 'Iranian Hacker Charged in HBO Hacking That Included 'Game of Thrones' Script' *The New York Times* (21 November 2017) <https://www.nytimes.com/2017/11/21/business/hbo-hack-charges.html> accessed on 9 March 2024

[63] 'Hackers Demand Millions in Bitcoin for Stolen HBO Files' *The New York Times* (7 August 2017) <https://www.nytimes.com/2017/08/07/business/hackers-demand-ransom-for-stolen-hbo-files.html> accessed 09 March 2024

[64] Ben Knight 'Cyberattack knocks out major news group' *DW* (29 December 2020) <https://www.dw.com/en/germany-colossal-cyberattack-knocks-out-funke-news-group/a-56087804> accessed 07 March 2024

[65] *Ibid*

OBSERVATIONS FROM THE ABOVE CASES

The above cases and regulatory frameworks signify an ongoing process to understand the need for privacy legislation and cybersecurity measures in the entertainment and media industries. The cases highlight several human fallacies that put the personal data of consumers, the company's internal documents, and their own employees' data at potential risk of being stolen or misused by cybercriminals.

Cybercriminals often use data breaches as a method to either fulfil a negative personal vendetta or for purely financial motivation (extortion and ransom). As seen in the case of HBO (2017), the data breach was engineered by an experienced ex-military hacker (from Iran) to extort a ransom of $6 million in Bitcoin.

It can also be observed that the board members or the core management of these companies are prone to cost-cutting in taking cybersecurity measures, which often backfires and increases their costs in litigation, penalties, loss of customer trust, and damage to their brand name and reputation. In the case of Ashley Madison, the company lied about its privacy and data retention policies. The company provided the users with a false sense of security, that on payment for deletion of their data from their database, it would be permanently deleted. Later, during an investigation for a potential data breach, it was found that the data was never permanently deleted. This caused the customers mental and reputational agony, with several of them resorting to extreme measures, such as committing suicide.

The legislation needs to be flexible and amended at regular intervals to integrate new approaches to crisis scenarios. It can be seen that most countries don't draft their legislation to accommodate futuristic problems.

THE WAY FORWARD

Data breaches not only involve breaches of privacy but also include breaches of other aspects of legal compliance, such as cyber legislation, rights of consumers, and financial laws. The lack of adequate risk mitigation can be more detrimental and costly than the cost of legal compliance

and the implementation of data protection laws.[66] Here are certain suggestions to understand and prevent such data breaches and cybercrimes as much as possible:

Addressing Piracy: Piracy in the entertainment industry needs to be addressed separately and strictly. The measures regarding piracy should be proactive in curbing the supply of pirated products to consumers on various online forums ranging across different digital formats. A great example of piracy control is Germany.[67] The laws about such acts are strict, and the individuals found indulging in such acts are imposed with hefty fines. And for serious violations, there can be a penalty involving a prison sentence.

Adoption of Data Governance Policies: Establishing clear policies within entertainment and media companies for data collection, storage, access, and disposal is vital. These policies minimise unauthorised access and misuse, potentially minimising the cost of data breaches incurred by the companies, IBM's Cost of a Data Breach Report 2023 reported an average cost of $4.45 million per data breach.[68]

Invest in Employee Awareness and Education: Employees are the soul of any company. Focusing on their training, organising awareness workshops, and creating an amiable environment for complying with privacy regulations should be the goal of companies today. It is estimated that 74% of all breaches are a direct result of a lack of employee awareness.[69] To ensure data security, empowering an employee with knowledge of privacy and caution towards potential cybersecurity risks can help in the long run. To successfully evaluate a phishing scam, maintaining password hygiene, and handling data in a legally compliant manner can reduce the percentage of employees falling victim to such factors due to a lack of awareness.

---

[66] Ed Goldberg, 'Preventing a Data Breach From Becoming a Disaster' (2013) 6(4) Journal of Business Continuity & Emergency Planning 295-303 <https://www.researchgate.net/publication/247771452_Preventing_a_data_breach_from_becoming_a_disaster> accessed 07 March 2024

[67] Darko Janjevic, 'Internet Pirates walk a fine line in Germany' *DW* (11 November 2016) <https://www.dw.com/en/internet-pirates-walk-a-fine-line-in-germany/a-36364095> accessed 07 March 2024

[68] 'Cost of a Data Breach Report 2023' (*IBM*, 2023) <https://www.ibm.com/reports/data-breach> accessed 07 March 2024

[69] Madhur Chaturvedi 'Human Element Remains Biggest Threat: Verizon's 2023 Data Breach Investigations Report' *NDTV Profit* (23 August 2023) <https://www.ndtvprofit.com/technology/human-element-remains-biggest-threat-verizons-2023-data-breach-investigations-report> accessed 05 March 2024

Regular Checks and Assessments: The companies should conduct regular vulnerability assessments. There should be a focus on regularly updating software, databases, passwords, and systems. The 2024 IBM Security X-force Threat Intelligence Report stated an increase of 32% in cyberattacks was linked to data theft and leaks.[70] This indicates a rising trend of stealing and selling data.

Crisis Management Plan: In case of a cyber-attack, the entertainment and media companies need to have a prompt response plan to tackle the attack. There needs to be an internal team dedicated to handling breach notifications to authorities and customers, media statements, and engineers to quickly de-escalate the cyber-attack damage.

CONCLUSION

In conclusion, it can be said that the legal implications of data breaches in the entertainment and media industry are a call for help and highlight the need for robust privacy frameworks. There needs to be efficient implementation of privacy compliance frameworks like the GDPR and regional legislations across the globe supplemented by a well-oiled enforcement authority.

It is important to understand that data privacy and data security are parallel paths leading to compliance with the complex legal landscape. Data breaches have affected every possible industry globally, yet there is a need for robust cybersecurity measures, compliance with privacy regulations, and active as well as aware employees of such industries that are the actual line of defence. It is the continuous cycle of identifying new aspects and methods of security, vigilance, and adaptability that hold the key to protecting valuable personal and sensitive data.

Data breaches leave a profound impact on companies and customers alike. The repercussions range from financial loss and reputational damage to erosion of customer trust and the burden of legal lawsuits unveils a grim picture of lacklustre management and unserious implementation and compliance with cybersecurity measures.

[70] 'IBM X-Force Threat Intelligence Index 2024' (*IBM*, 2024) <https://www.ibm.com/reports/threat-intelligence> accessed 07 March 2024

Therefore, the possible solution for such a problem is through rigorous legal compliance, implementation of safety measures and ensuring a humane approach to customer data. The fundamental principle of privacy law is to protect the affected individual from further repercussions while fostering a sustainable, proactive and holistic (or humane) approach to addressing such delicate issues regarding their data being leaked, hacked or sold.