

ISSN: 2582 - 2942



LEX FORTI

LEGAL JOURNAL

VOL- I ISSUE- VI

AUGUST 2020

DISCLAIMER

No part of this publication may be reproduced or copied in any form by any means without prior written permission of Editor-in-chief of LexForti Legal Journal. The Editorial Team of LexForti Legal Journal holds the copyright to all articles contributed to this publication. The views expressed in this publication are purely personal opinions of the authors and do not reflect the views of the Editorial Team of LexForti. Though all efforts are made to ensure the accuracy and correctness of the information published, LexForti shall not be responsible for any errors caused due to oversight otherwise.



ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR IN CHIEF

ROHIT PRADHAN

ADVOCATE PRIME DISPUTE

PHONE - +91-8757182705

EMAIL - LEX.FORTII@GMAIL.COM

EDITOR IN CHIEF

MS.SRIDHRUTI CHITRAPU

MEMBER || CHARTED INSTITUTE
OF ARBITRATORS

PHONE - +91-8500832102

EDITOR

NAGESHWAR RAO

PROFESSOR (BANKING LAW) EXP. 8+ YEARS; 11+ YEARS WORK EXP. AT ICAI; 28+ YEARS WORK EXPERIENCE IN BANKING SECTOR; CONTENT WRITER FOR BUSINESS TIMES AND ECONOMIC TIMES; EDITED 50+ BOOKS ON MANAGEMENT, ECONOMICS AND BANKING;

EDITOR

DR. RAJANIKANTH M

ASSISTANT PROFESSOR (SYMBIOSIS INTERNATIONAL UNIVERSITY) - MARKETING MANAGEMENT

ISSN: 2582 - 2942

EDITORIAL BOARD

EDITOR

NILIMA PANDA

B.SC LLB., LLM (NLSIU) (SPECIALIZATION BUSINESS LAW)

EDITOR

DR. PRIYANKA R. MOHOD

LLB., LLM (SPECIALIZATION CONSTITUTIONAL AND
ADMINISTRATIVE LAW)., NET (TWICE) AND SET (MAH.)

EDITOR

MS.NANDITA REDDY

ADVOCATE PRIME DISPUTE

EDITOR

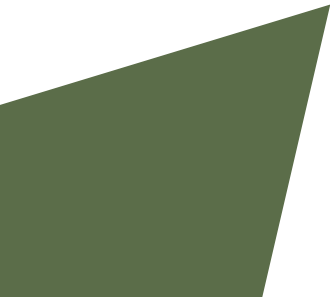
MS.SRISHTI SNEHA

STUDENT EDITOR



ABOUT US

LexForti is a free open access peer-reviewed journal, which gives insight upon broad and dynamic legal issues. The very objective of the LexForti is to provide open and free access to knowledge to everyone. LexForti is highly committed to helping law students to get their research articles published and an avenue to the aspiring students, teachers and scholars to make a contribution in the legal sphere. LexForti revolves around the firmament of legal issues; consisting of corporate law, family law, contract law, taxation, alternative dispute resolution, IP Laws, Criminal Laws and various other Civil issues.



Tort of Misuse of Private Information

Pranay Bharadwaj

INTRODUCTION

1.1 CONTEXT-

The 21st century has witnessed the meteoric rise of data harvesting and analysis techniques, with jobs in data extraction and dissection increasing five folds from the year 2000 to 2010¹. These jobs involve accessing the private information of persons online, without their consent, and using it for undisclosed purposes.

Recently it was revealed that in the 2016 US election, a company called Cambridge Analytica had used such techniques to gain access to the private information of 87 million American Facebook users without their authorization and analyzed it to micro-target US voters with pro-Trump messages tailored according to each individual's online behavior². Similar accusations have been made against the company by the Indian and the British government in the context of the 2014 Indian elections and the 2016 Brexit referendum.

If such reports are confirmed in the case of the Brexit referendum, British citizens will have a tort remedy available to them, called- "misuse of private information." However, affected users in US and India will be left with no legal recourse.

Given these developments, the relevance of this newly formed tort has dramatically increased. However, its significance has been largely neglected in Indian academic and judicial discourse. Thus, the researcher has chosen it as the subject for his analysis. The rise of data harvesting, the recent willingness of political campaigns to use it and the lack of other legal recourses in such situations, necessitate a closer study of this tort, as a possible measure to counter these trends and ensure legal accountability for unscrupulous actors.

1.2 STRUCTURE

This paper will begin with a description of the origin of the tort under discussion, both in terms of precedent and theory, and will give several reasons in favor of its categorization as a tort separate from the equitable wrong of "breach of confidence" in the United Kingdom. These reasons will include its inadequacy, the possible jurisdictional issues posed by it and its outdated nature. It will then explain the test currently used by English courts to determine if an act amounts to "misuse of private

¹ Forbes.com. (2019). A Very Short History Of Data Science. [online] Available at: <https://www.forbes.com/sites/gilpress/2013/05/28/a-very-short-history-of-data-science/#7beb19db55cf> [Accessed 5 Oct. 2019].

² Nast, C. (2019)." Facebook Exposed 87 Million Users to Cambridge Analytica. [online] Wired. Available at: <https://www.wired.com/story/facebook-exposed-87-million-users-to-cambridge-analytica/> [Accessed 5 Oct. 2019].

information' and the extraneous factors that the courts consider while applying this test. It will then argue that Indian courts must also develop a new tort of 'misuse of private information' and list the combination of factors that make it necessary.

RESEARCH METHODOLOGY

This paper will limit its scope to the legal systems of India, the United States and England. Separate categorization of closely linked and vaguely defined torts in the field of privacy and differences in privacy clauses of the national and international laws of the 3 countries will pose a procedural challenge to the research. However, it will be dealt with, by operating with the most widely accepted and recent interpretations of these laws and by focusing on the substantive commonalities in the privacy laws of all three nations.

The legal sources will include judicial decisions, statutes, the Indian constitution and peer reviewed academic publications. Sources on technical aspects of data harvesting and trading will include newspaper articles and published commentaries by qualified experts in the field.

The paper will pose and attempt to answer the following 2 questions-

1. What is the origin of the tort of “misuse of private information”?
2. Should a separate tort of “misuse of private information” exist in the Indian context?

Each of the aforementioned questions will be answered in detail with reference to considerations of public policy, existing regulations, trend of judicial decisions, effectiveness of privacy torts till now and the urgency of the matter, given the current data harvesting situation.

OVERVIEW AND ANALYSIS

3.1 ORIGIN

‘Misuse of private information’ was established as a separate tort by the United Kingdom’s Court of Appeal in 2004, in the case of *Campbell v Mirror Group Newspapers Ltd*³. Prior to this, the claim was classified solely as a violation of article 8 of the European Human Rights Convention⁴, enforceable against both the state and private persons in the United Kingdom, through ‘The Human Rights Act’, 1998⁵. In order to understand the importance of its classification as a “tort”, we must briefly discuss the case of *Vidal-Hall v Google Inc.*⁶ that reaffirmed this classification. We must appreciate the jurisdictional issue faced by the court in this case and comprehend why this issue would have been faced by the courts on a regular basis ,if this tort classification wasn’t followed.

The problem in this case, and many others involving American Tech companies, was that as Google Inc.’s registered office was located in Delaware, United States (a non-European Union state), English courts couldn’t enforce article 8 of EHRC against it through an injunction unless the claim was proved to be within the ambit of a particular “jurisdictional gateway” listed in England and Wales’ Civil Procedure Rules (1998)⁷.

A claim under an “equitable wrong” like Breach of confidence law does not count as a “jurisdictional gateway”, but a claim under “tort” does, according to the authority of *Kitechnology BV v Unicor GmbH Plastmaschinen*⁸. Thus, to assert its jurisdiction over Google Inc. and dispense justice in this matter, the court decided to uphold the classification of the claim of “misuse of private information” as a tort.

The court gave three main reasons for its judgement. Firstly, ‘misuse of private information’ is a tort distinct from the equitable wrong of breach of confidence as they endeavor to protect different legal interests. The former seeks to protect the individual’s right to privacy and prevent dissemination of information not intentionally divulged to anyone, whereas the latter seeks to prevent dissemination of confidential information, originally shared willingly to the defendant, making the former much graver than the latter and worthy of classification as a tort. Secondly, the court found no reason based on public policy or principle that made an alternative classification more appropriate. Thirdly, the court

³ *Campbell v Mirror Group Newspapers Ltd* [2004] UKHL 22

⁴ Art. 8, ECHR

⁵ The Human Rights Act, 1998 (c42)

⁶ *Vidal-Hall v Google Inc.* Reference: [2014] EWHC 13 QB)

⁷ UK: Civil Procedure Rules (1998)

⁸ *of Kitechnology BV v Unicor GmbH Plastmaschinen* [1995] FSR 795

noted that the House of Lords referred to the claim of “misuse of private information” as a tort in multiple judgements like *OBG Ltd v Allen*⁹, *McKennitt v Ash*¹⁰ and *Imerman v Tchenguiz*¹¹, with the sole exception of *Douglas v Hello!*¹². We must note here that there exists no general right to privacy under English common law and thus, no other, more comprehensive form of tort claim could have been made in this instance.

We must also note that this tort’s judicial recognition was preceded by its academic theorization. Lord Nicholls of Birkenhead himself, in his judgment on the Campbell case, cited a legal scholar named Gavin Phillipson, and his article “Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act” (2003)¹³, which argued in favor of recognizing a right to privacy, separate from a right to confidence. Theoretically speaking, each tort requires the existence of a duty of care and some damage caused by the breach of that duty. Legal Scholars like Phillipson argued that just as business associates have a “duty of confidentiality” towards each other; commonplace individuals that lack an initial relation of confidentiality, have a “duty of privacy” towards one another in light of values enshrined in article 8 of European Convention on Human Rights. They pointed to the judgement of Lord Goff of Chieveley in the case of *Attorney-General v Guardian Newspapers Ltd*¹⁴ that pointed out this distinction in its obiter. This distinction is what leads Lord Nicholls to observe that “An individual’s privacy can be invaded in ways not involving publication of information” .The damage also need not be pecuniary, instead, much like trespass , the voluntary violation of the legal right to privacy is considered to be a form of damage in itself.

To understand the international relevance of this tort without exceeding the research’s scope, we must mention (without elaboration) that based on the Campbell case, common law countries like Canada and New Zealand have included claims of misuse of private information in their pre-existing tort of ‘invasion of privacy’.

3.2 CURRENT TESTS AND REQUIREMENTS

The test used in UK courts currently for determining the existence of liability in claims of ‘misuse of private information’ is the 2 stage test laid down in the case of *Vidal-Hall v Google Inc.*¹⁵.

⁹ *OBG Ltd v Allan* [2007] UKHL 21

¹⁰ *McKennitt v Ash* (CA). Reference: [2006] EWCA Civ 1714

¹¹ *merman v Tchenguiz* ([2010] EWCA Civ 908)

¹² *Douglas v Hello! Ltd* [2005] EWCA Civ 595

¹³ Gavin Phillipson, *Transforming Breach of Confidence? Towards a Common Law Right of Privacy under the Human Rights Act*, 66 *Modern Law Review* 726-758 (2003) .

¹⁴ *Attorney-General v Guardian Newspapers Ltd* CA ([1988] 2 WLR 805)

¹⁵ *ibid*

The first stage involves checking if there was a reasonable expectation of privacy for the information in question. The UK Supreme Court, in the case of *David Murray v Big Pictures (UK) Ltd.*¹⁶, prescribes the criteria for identifying the existence of such a reasonable expectation. The criteria includes the nature of activity, its place, the consent (explicit or implicit) of the plaintiff, nature and purpose of intrusion by defendant, the effect on the plaintiff, and the circumstances and purpose for which the information was transferred to the publisher.

If the claimant passes the first stage, the court will engage in a balancing exercise between the free speech rights of the publisher given in article 10 of ECHR and the privacy right of the person in question given in article 8 of the ECHR. Lord Steyn also laid down 4 principles which must be taken into consideration by the courts while performing this exercise, in the *Campbell* case. These principles are- Neither of these rights takes precedence over the other, the court must focus on the comparative importance of the competing claims in terms of public interest, the court must hear the justifications for invading each right and the court must apply the 'proportionality test' and check whether the violation of right was significant enough for a tort claim.

The second principle that emphasizes the relevance of 'public interest' in the balancing exercise has been derived from previous UK tort cases like *Max Mosley v Newsgroup Newspapers Ltd.*¹⁷ and European court of human rights cases like *Von Hannover v Germany*¹⁸ that drew a distinction between reporting of facts that will contribute to a debate relating to "politicians in the exercise of their functions" and reporting of facts that does not. Cases in which the published information contradicts the image advanced by the claimant will also be considered to be in public interest, according to the same authority.

3.3 NECESSITY IN INDIA

The requirement of the tort of "misuse of private information" emanates from the combination of 3 factors- the rise of social media and data harvesting, the lack of data privacy laws and the usual lack of a contractual relationship between the user and the entity harvesting the user's data. This paper will now discuss them in detail, and incrementally build its argument for the tort's establishment in India.

¹⁶ *Murray v Big Pictures (UK) Ltd* [2008] EWCA Civ 446

¹⁷ *Mosley v News Group Newspapers Ltd.* [2008] EWHC 1777 (QB)

¹⁸ *Von Hannover v Germany*: ECHR 24 Jun 2004

3.3.1 THE RISE OF SOCIAL MEDIA AND DATA HARVESTING

In order to understand the need for the tort of “misuse of private information” in India, we must take note of the rise of social media companies in the country, both in terms of their user bases and their political influence.

Facebook has more than 241 million active users in India, the highest number in any country.¹⁹ Given that only 19 % of Indians currently use social media platforms²⁰, as compared to nearly 50% of Indians that have access to the internet²¹, the company still has significant potential to grow in the nation. Similarly, other social media platforms like Instagram and snapchat are also looking to aggressively expand their user bases in India.

The way in which these companies earn their revenue is what makes their rise relevant to the development of the tort under discussion. These companies sell the data of their users to corporate advertisers. This includes information about their user’s interests, religion, political affiliation, sexual orientation etc. and is generally used by these corporations for targeted advertising. Social Media companies also allow software developers to let its users opt for the app through their Facebook account. This lets them access information about not just the person who used the software, but also all the Facebook friends of this individual, without their consent. As mentioned in the introduction, firms like Cambridge Analytica have used the latter technique to harvest the data of eligible voters and subject them to targeted political advertisements in various regional Indian elections according to the Central Bureau of Investigation²². Moreover, given that the primary source of news for 68% of Indians is their mobile phone²³, the influence of websites like Facebook on Indian political discourse is significant.

Thus, given the exponential increase in user base of social media companies, the data selling they engage in and the massive political implications that the transfer of this data has, there is an urgent

¹⁹ Donna Fuscaldo, Facebook Now Has More Users in India Than in Any Other Country Investopedia (2019), <https://www.investopedia.com/news/facebook-now-has-more-users-india-any-other-country/> (last visited Oct 6, 2019).

²⁰ *ibid*

²¹ Internet users in India to reach 627 million in 2019: Report, The Economic Times (2019), <https://economictimes.indiatimes.com/tech/internet/internet-users-in-india-to-reach-627-million-in-2019-report/articleshow/68288868.cms?from=mdr> (last visited Oct 6, 2019) .

²² CBI writes to Facebook, Cambridge Analytica over data theft, The Economic Times (2019), <https://m.economictimes.com/news/politics-and-nation/cbi-writes-to-facebook-cambridge-analytica-over-data-theft/articleshow/65843687.cms> (last visited Oct 6, 2019).

²³ 68% of Indian users consume news on smartphones: Report | India News - Times of India, The Times of India (2019), <https://timesofindia.indiatimes.com/india/68-of-indian-users-consume-news-on-smartphones-report/articleshow/68565146.cms> (last visited Oct 6, 2019).

need for the development of a legal framework to hold these companies accountable, if their practices compromise the privacy of their users without their consent.

3.3.2 LACK OF COMPREHENSIVE DATA PRIVACY LAWS

India has no explicit data protection legislation in force at the moment. However, various laws and bills address data privacy in particular contexts. Section 43A of The Information Technology Act 2000²⁴ offers protection for “sensitive personal data” like bank account details and place of residence by compelling any “body corporate” to compensate any user that faces “wrongful loss” due to their negligent security practices.

The Sensitive Personal Data or Information rules, 2011²⁵, notified by the government under the aforementioned act prohibit further transfer of “sensitive data” by the private entity that originally received it by the consent of the user. The government has also proposed expanding the scope of this section to include public entities. We must note that these rules apply only to body corporates and persons located in India. According to these rules, all such body corporates must obtain the consent of the data principal before processing his data and publish the purpose of the data processing and their privacy policy in clear terms on their website. They mandate that the body corporate undertakes “reasonable security practices” to protect the data and that the data must be retained only until it is needed for the stated purpose. It also provides for the establishment of a “grievance office” that will address the complaints of data principals within one month of their filing and audit the security practices of data processors at least once a year in general and specifically when it upgrades its “computer resources” and processes. Any disclosure of such personal data in breach of a contract entered into for obtaining the said data will lead to imprisonment for three years or a fine of rupees 50 lakhs or both.

Indian citizens also have a fundamental right to privacy under article 21 and article 19 of the constitution²⁶ according to Justice K. S. Puttaswamy (Retd.) and Anr. vs Union Of India And Ors²⁷, but it can generally be enforced only against the state and not against private entities.

²⁴ The Information Technology Act, 2000, no. 21, Acts Parliament, 2000 (India)

²⁵ Sensitive Personal Data or Information rules, notified by Indian govt. in 2011, under The Information Technology Act, 2000

²⁶ INDIA CONST .art 21, art.19

²⁷ Justice K.S. Puttaswamy v. Union of India) (2017) 10 SCC 1.

India has also ratified the International Covenant on Civil and Political Rights²⁸, which guarantees all individuals the right against arbitrary or unlawful invasion of privacy under article 17. However, non-arbitrary invasion of privacy for one's own gain isn't explicitly prohibited by it.

As per the recommendations of the BN Srikrishna Committee, the Ministry of Electronics and Information Technology has also drafted a new data privacy bill called The Personal Data Protection Bill, 2018²⁹. This bill requires that both private and public entities process data in a "fair and reasonable"³⁰ manner and notify the user or the "data principal" about the nature and purpose of their data processing. The kind of conduct that will be considered "fair and reasonable" will be a function of the scope of consent given by the user. If data fiduciaries (entities processing the data) don't comply with these requirements, they will be subjected to a fine of up to 15 crore rupees or 4 percent of its total worldwide revenue (whichever is higher). The bill also endows the data principal with the right to seek access or correction to their data and sets up a "Data protection Authority" to regulate and supervise data fiduciaries in order to ensure compliance. Moreover, it compels data fiduciaries to report any breach of data to the DPA, if it's likely to cause harm to the data principal, failing which it will be liable to pay a fine of up to 5 crores or 2% of its total worldwide revenue (whichever is higher).

Nevertheless, the bill makes an exception for entities processing data that is needed for journalistic research, national security purposes and legal proceedings, which can still be collected without the data principal's consent.

These facts often lead critics to contend that the tort of 'misuse of private of information' is unnecessary'. This counter argument is flawed in several respects. At the very outset, we must keep in mind that similar bills have been proposed by the government since 2009 but none of them have turned into law. The setting up of the Data Protection Authority might take several years, even if it were to pass. Moreover, even if we were to assume that this bill will be passed, and that the DPA will be swiftly established, there are several major data privacy issues that this bill fails to address. Firstly, the legislation seeks to protect "personal information" and not "private information". This distinction is extremely significant as the former refers to any information that renders an individual specifically identifiable, whereas the latter refers to information regarding which a person can have a reasonable

²⁸ International Covenant on Civil and Political Rights, entry into force 23 march, 1976, United Nations, Treaty Series, vol. 999, p. 171.

²⁹ Personal Data Protection (draft) Bill, 2018

³⁰ Personal Data Protection (draft) Bill, 2018, Art. 4

expectation of privacy. This means that information about a person's political affiliations, religion or sexual orientation, when clubbed into a class such that it can't be used to specifically identify a particular person, won't be protected by this law at all, rendering the law futile in terms of dealing with data harvesting by political campaigns. Secondly, the legislation gives no guidelines regarding what kind or processing would be considered "fair and reasonable" and what type of breach are likely cause "harm" to the data principal. This means that the fairness and reasonableness of the data processing and the likelihood of harm resulting from a data breach will be left to the discretion of the data fiduciary, creating scope for abuse and making it harder to prove their non-compliance with the law. This abuse is likely to occur as there is a clear conflict of interest. If the data fiduciary is a corporation, reporting data breaches may lead to a decline in their stock price and their reputation in the market and if it is a government entity, it may lead to the public humiliation and firing of the person in charge of it, which creates a perverse incentive to not report such breaches. Thirdly, exemptions provided to entities processing data for journalistic research, the functioning of the parliament and any state legislature and for legal proceedings are rather unfounded, unlike the exemption for national security. These exemptions would allow firms like Cambridge analytica to obtain data by claiming that the purpose of their data processing is journalistic political research, and would permit them to furnish the conclusions of their research to a political campaign, as long as they don't furnish the raw data itself. Fourthly, a complaint may be raised by the data principal against a data fiduciary only if a provision of the bill has been violated and if this violation has caused harm or is likely to cause harm. Thus, the violation of the right to privacy itself is not sufficient to raise a complaint. This means that even if the data of an individual is taken without his consent, he would have no legal recourse against the perpetrator, unless he can prove that the harvesting of his data has led to or is likely to lead to any harm.³¹

Thus, both the existing laws, like the Information technology Act, 2008 and the SPDI rules and the bill proposed by the government, fail to include non-personal private information in their ambit, give data fiduciaries excessive discretion in deciding the reasonableness of their data processing practices and fail to compensate data principals for violation of their privacy, if the said violation does not or is not likely to, cause any harm. Moreover, we must keep in mind that the new bill may not even be introduced in the parliament, like all of its predecessors. Thus, we can infer that India has a grave lack

³¹ Draft Personal Data Protection Bill, 2018, PRSIndia (2019), <https://www.prsindia.org/billtrack/draft-personal-data-protection-bill-2018> (last visited Oct 6, 2019).

of legal provisions protecting data privacy and that this situation is likely to continue for the foreseeable future.

3.3.3 RELATIONSHIP BETWEEN USER AND DATA HARVESTING ENTITY

In the vast majority of cases involving data harvesting, the user has no direct contractual relationship with the entity harvesting his data. In order to comprehend how this is possible, we must engage in an in-depth analysis of the various contractual relationships involved in the Cambridge analytica scandal.

All Facebook users had a contractual relationship with Facebook, emanating from their required agreement to Facebook's terms of service. An additional contractual relationship existed between Facebook and Cambridge analytica, according to which Facebook would allow Cambridge analytica to give its users the option to login to their app called "thisisyourdigitallife" through their Facebook accounts³². The users of this app had a contractual relationship with Cambridge analytica, by virtue of their agreement to the company's own Terms of service. This included a permission to access not only their private information, like pictures, private posts and messages, occupational status etc. but also that of everyone in their friend list. The friends of these users had not consented to giving up their private information to Cambridge Analytica, and were not even informed of this transfer of data. Thus, there existed no contractual relationship between these persons and Cambridge Analytica, but the latter was still able to access the former's information without hacking their account. This information was then analyzed and offered to Trump's Presidential Campaign.

The lack of a contractual relationship meant that these persons couldn't sue Cambridge analytica for 'breach of contract' when they furnished their private information to the Trump campaign, under both American and Indian laws. Given that the company didn't hack their accounts, a tort claim under America's Computer Fraud and Abuse Act, 1986³³ or section 66 of India's Information Technology Act, 2000³⁴ would also not be entrained by the courts in the respective countries. A claim under the American tort of 'invasion of privacy' or the Indian tort of 'breach of confidentiality' would also have

³² Kurt Wagner, Here's how Facebook allowed Cambridge Analytica to get data for 50 million users Vox (2019), <https://www.vox.com/2018/3/17/17134072/facebook-cambridge-analytica-trump-explained-user-data> (last visited Oct 6, 2019) .

³³ Computer Fraud and Abuse Act, 18 U.S. Code § 1030 (1986)

³⁴ *ibid*

failed legal scrutiny. In order to understand the reason behind this, these torts must be discussed in further detail.

Invasion of privacy claims are of 4 main types- “Appropriation of name or likeness”, “intrusion upon seclusion”, “false light” and “public disclosure of private facts.” Given that Cambridge Analytica didn’t hijack anyone’s identity, the first type of this tort won’t be applicable. Given that the data principals in this case were not “secluded”, or in a state of solitude, the second type of this tort also won’t apply. Given that the firm did not leak any “potentially misleading” or “damaging” information about the data principals, the third type of this tort also wouldn’t apply. Given that the firm didn’t publicly disclose any of the data harvested by it, the fourth type of this tort will also not be applicable.³⁵ The tort of breach of confidence only applies to information that is originally disclose willingly and is furnished to a third party, without the subject’s authorization, according to the authority of *Ansell rubber Co. Pvt. Ltd v Allied Rubber industries Pvt. Ltd.*³⁶. Given that the data was never communicated willingly to Cambridge Analytica, this tort would also not apply.

Thus, due to the lack of any contractual relationship between the data harvester and the data principal; and the nature of the method used to harvest the relevant data, no tort or crime could have been used to hold the data harvester accountable, under American or Indian law , except for that of ‘misuse of private information’.

It’s imperative for the law to keep up with the technological advances in society and for the court to not let grave violations of privacy continue while the public awaits legislative or executive action. In light of the widespread data harvesting in the current social media scenario, the inadequacy of the current data privacy laws like The information Technology Act (2000)³⁷, the SDPI rules, the new Personal Data Protection Bill,2018³⁸ ,the torts of breach of confidence and the fundamental right to privacy under article 21 and 19³⁹ and the usual lack of any contractual or proximate relationship between the data principal an the data harvester, this paper answers its second research question in the affirmative- Indian courts must introduce a new tort of ‘misuse of private information’.

³⁵ What Is Invasion of Privacy?, Findlaw (2019), <https://injury.findlaw.com/torts-and-personal-injuries/what-is-invasion-of-privacy-.html> (last visited Oct 6, 2019) .

³⁶ *Ansell Rubber Co Pty Ltd v Allied Rubber Industries Pty Ltd* 1967 VR 37

³⁷ *ibid*

³⁸ *ibid*

³⁹ *ibid*

CONCLUSION

This research paper began by providing the political and technological context that necessitated a discussion on the tort of ‘misuse of private information. It then laid out the structure of its content and arguments. It mentioned the rapid rise of data harvesting and social media and the establishment of firms like Cambridge Analytica to demonstrate the pressing nature of the matter. It went on to describe the research methodology employed by it and specified its scope, sources and the two questions it intended to answer. The first concerned the origin of the tort of ‘misuse of private information’ and the second was regarding whether the tort should be introduced in the Indian legal system.

The paper then proceeded to answer the two questions posed by it. It explained how the tort was initially recognized in the United Kingdom in the case of *Campbell v Mirror Group Newspapers Ltd.*⁴⁰ and reaffirmed in the case of *Vidal-Hall v Google Inc.*⁴¹ It also elucidated the jurisdictional issue relating to US based companies like Google, which this classification solved. It then discussed the 2 stage test currently employed by English courts to determine if a piece of information is ‘private’ and if a particular way of dealing with it constitutes ‘misuse’. The requirement of ‘reasonable expectation of privacy’ and the balancing of the individual’s right to privacy against the publisher’s right to free speech and expression was explained.

The paper then went on to answer its second question in the affirmative, and argued that Indian courts must also recognize a tort of ‘misuse of private information’. It contended that a combination of three factors made this act an absolute necessity and articulated each of them in detail. These included the rise of social media and data harvesting, the lack of comprehensive data privacy laws in the country and the usual lack of any contractual relationship between the data principal and the data harvester.

The researcher has observed that the Indian courts have been willing to develop new torts if the existing legal regime fails to protect a particular right of the citizens, in accordance with the principal of ‘*ubi jus ibi remedium*’ laid down in the case of *Ashby v White*⁴². The development of the tort of ‘Breach of Confidence’ in the case of *Zee Telefilms Limited and Another Vs. Sundial Communications*

⁴⁰ *ibid*

⁴¹ *ibid*

⁴² *Ashby v White* (1703) 92 ER 126

Private Limited and Other⁴³s perfectly exemplifies this tendency. Thus, the researcher would like to conclude this paper by contending that recognizing a tort of ‘misuse of private information’ would constitute a mere continuation of this pre-existing trend of Indian jurisprudence, and would prove to be a vital step towards protecting the modern Indian citizen’s right to data privacy.

⁴³ ZEE Telefilms Ltd. V Sundial Communications 2003 (27) PTC 457