
PRIVACY AND DATA PROTECTION IN CYBERSPACE

Ms. Bhumika Dandona, Student, BBA-LLB(H.), Sushant University, Gurugram, Haryana.

ABSTRACT

Everyone has heard of the term 'cyberspace' in this age of technology. It refers to a virtual world, interconnected by several computers or computer networks, that allows everyone to communicate with one another, play games, watch videos, text, and much more. While it is worth appreciating, this digital area has many bad points about it as well. It is a known fact that cyberspace is a breeding ground for criminals looking to acquire their selfish interests. Even though many indulged in such activities even before the advent of cyberspace, its introduction and gradual expansion could cause illegal chaos. Thus, it has to have some regulation. It was this view that led governments all around the world to introduce various legislation to regulate cyberspace.

Another problem with cyberspace is that of privacy. Privacy is a state of being able to seclude our thoughts, emotions, personal information, etc., and having an experience best known to ourselves. In India, privacy has become a fundamental right. Therefore, it needs protection. Privacy becomes easily vulnerable to violations in cyberspace these days. To combat the same, India has introduced various regulatory measures and laws.

Keywords: Cyberspace, privacy, fundamental rights, cybercrimes, and legislations.

Introduction

Cyberspace is a virtual reality that has completely changed how the world functions. Human beings have witnessed a gradual shift from physical to online events over the past few decades. Technology has partially replaced everything, from manual money transactions to in-person meetings and traditional learning, with digitization. But like what people always say, everything comes with its advantages and disadvantages. While the advent of cyberspace has made lives seamlessly easy, several other problems too arrived with it. One of those is the concern regarding the privacy of the citizens of cyberspace. If some people use technology to create a positive difference in society, others use it to commit unlawful acts.

Cybercrimes form a significant part of the news that we hear now and then. Instances of credit card theft and identity theft online are nothing new. It has led people to wonder about the safety of their privacy while surfing the Internet. Every person in India is entitled to the privacy of their personal information. Since it is a fundamental right, the Government must ensure that no one subjects it to a violation. Keeping in view the same, the Government brought about some codifications and rules in the last few years to minimize intrusion into people's privacy in the digital arena. These laws seek to regulate data protection in the country. However, the question is how effective they are to fulfill the purpose of their existence.

The Concept of Cyberspace

As per the Oxford Dictionary, cyberspace refers to the notional environment in which communication over computer networks occurs¹. It is a virtual world, interconnected by several computers or computer networks, that allows everyone to communicate with one another, play games, watch videos, text, and much more. People can do all these things sitting in one place, without having to make any physical effort. Thus, cyberspace enables people to function efficiently. It also eliminates geographical barriers, letting individuals interact with their fellow humans at the click of a button.

1. Backdrop in a nutshell

It was the American-Canadian author William Gibson who coined the term 'Cyberspace'. He first mentioned it in one of the local magazines during the early 1980s. Later on, the word found its way into his book *Neuromancer*. He defined cyberspace as a formation of computer

¹ The Oxford Dictionary, 10th Edition.

networks covering within its ambit artificially intelligent beings. This term became a popular modern slang in the 1990s for a place where people could connect through any online platform, such as the Internet.

In the initial years, cyberspace remained free from any regulation. However, soon governments across the globe began to ponder upon the lack of control over its use. Most of them believed that although a valuable field of technology, it was susceptible to misuse. The U.S. enacted the Digital Millennium Copyright Act, 1998, and other legislation to limit online activities to a reasonable extent. India formulated the Information Technology Act, 2000 to curb online crime rates. China maintains a strict constraint on who can have access to cyberspace and under what situations. Apart from that, institutions such as Electronic Frontier Foundation came up with the same intention.

Meaning of Privacy

Privacy means having control over one's affairs without any interference from the outside. It is a state of being able to seclude our thoughts, emotions, personal information, etc., and having an experience best known to ourselves. What one must note is that the term 'privacy' does not have a firmly secured definition. Different people have given their interpretations of this word within various declarations, books, conventions, agreements, etc. However, only a handful of them is commonly in use.

2. Popular global concepts of privacy

The Black's Law Dictionary defines privacy as the right to be let by oneself. It is the right of an individual to be devoid of unjustifiable public attention. Privacy also signifies the right to live without unwarranted interventions by others in matters wherein their presence is unnecessary².

Cambridge Dictionary states that privacy is the condition of being let alone or the right to keep our relationships and personal affairs confidential³.

As per Article 12 of the Universal Declaration of Human Rights, 1948, there should be no arbitrary interference in any individual's private space, including his family, home, reputation, and honour. In case any such action takes place, individuals have the right to protection by law

² The Black's Law Dictionary, 11th Edition.

³ The Cambridge Dictionary, 4th Edition.

against the same⁴. Article 17 of the International Covenant of Civil and Political Rights, 1966, affirms that no person shall be subject to unlawful or arbitrary intervention in his personal space, reputation, and honour⁵.

3. Evolution of privacy in India

The concept of privacy in India travels back to the period of the 2nd century. It is mentioned in the ancient metrical Dharmashastra texture tradition of Hinduism, as well as Hitopadesh texts. These ancient works governed the matters of the privacy of individuals. All of their personal affairs could not be subject to public disclosure under the laws laid down by such textual bodies. Even the then rulers had to obey the same and be respectful of the citizens' private lives.

Over time, the idea of privacy broadened in its ambit. As India gained independence from British rule, the Constituent Assembly began to work on the Constitution. During its making, some took up the matter of including privacy as a fundamental right. K.M. Munshi and B.R. Ambedkar, among others, advocated for such an inclusion. But they faced opposition from, particularly B.N. Rau and A.K. Ayyar because they were not willing to give privacy a constitutional status. They believed that it would impact the litigation process and investigation powers of the police. Both of them convinced the Advisory Committee to exclude privacy from the framework of the supreme law. They were successful in their attempts. Hence, the final draft of the Constitution had no right relating to privacy.

However, it eventually found its way to this body of laws through later judicial interpretations.

The judicial system of India first dealt with privacy as a right during the 1960s. In the case *Kharak Singh v. State of Uttar Pradesh*⁶, the Supreme Court invalidated a few provisions in the Uttar Pradesh Police Regulations and Police Act, 1861. These provided for domiciliary visits at night, tracking the movements of people and their periodic inquiries. The main question herein was whether these provisions violated the petitioner's fundamental rights. The highest authority in the Indian judicial system, in its verdict, asserted that although the Constitution does not explicitly provide privacy as a fundamental right, it comes under the purview of Article 21 (right to life and personal liberty)⁷. It further upheld the recognition of privacy as a right

⁴ Universal Declaration of Human Rights, 1948 § Art. 12.

⁵ International Covenant of Civil and Political Rights, 1966 § Art. 17.

⁶ *Kharak Singh v. State of Uttar Pradesh*, 1963 AIR 1295, 1964 SCR (1) 332.

⁷ Legal Service India, <http://www.legalserviceindia.com/legal/article-276-evolution-of-right-to-privacy-in-india.html> (last visited Apr. 5, 2021).

under the common law. In the case *Govind v. the State of Madhya Pradesh*⁸, the principal issue was regarding the constitutionality of domiciliary visits by the police, as provided under the Madhya Pradesh Police Regulations. The Supreme Court held that such actions should only be applicable in situations wherein there is a danger to the community's interests. Otherwise, privacy invading provisions shall be unconstitutional.

Several other case laws imply the above-stated Supreme Court rulings regarding the right to privacy. But the most important of all these was that of *Justice K.S. Puttaswamy (retired) v. The Union of India and Ors*⁹. In 2017, a former judge of the High Court assailed the lawfulness of the Aadhar card. He contended in his petition that it caused a grave violation of the right to privacy, citing that the Supreme Court had delivered judgments on similar circumstances. The creation of such documents required the citizens to provide their personal information to the concerned authority. It could lead to the rise of a potential surveillance state. The respondents argued that the citizens did not have to submit all their details for the purpose in question. The sole motive behind the Aadhar card was to ensure that the maximum number of people avail of government benefits and services. After hearing the respective parties, the Supreme Court held that the Central Government did not violate any fundamental right. The nine-judge bench also put forth its views on the right to privacy. It recognized privacy as a right under Article 21 of the Constitution and made it clear that it is an incident of the right to life and personal liberty. Because it forms a part of human dignity it is a right conferred on individuals just by the virtue of being human.

Thus, with the emergence of different understandings given by the Indian courts, privacy gradually evolved as a fundamental right. Violation of the same would attract the operation of the relevant provisions under the Constitution.

Crimes In Cyberspace and Threats to Privacy

Crimes that take place through the use of computer networks or any online platform are called cybercrimes. Also known as e-crimes or information-age crimes, the word 'cybercrime' is the creation of renowned legal professors, Sussman and Heuston. The most distinct feature of these unlawful acts is that they do not require physical attempts to be in effect. Along with that, the efficiency of information technology also makes things much simpler for cyber criminals. Thus,

⁸ *Govind v. State of Madhya Pradesh*, 1975 AIR 1378, 1975 SCR (3) 946.

⁹ *Justice K.S. Puttaswamy (retired) v. The Union of India and Ors.*, (2017) 10 SCC 1.

with the advancement of cyberspace, there has also been a drastic increase in the number of cybercrimes. It has led to a threat revolving around the privacy of individuals, causing worry amongst everyone, including the authorities under the law and order system. Over the years, tech experts have categorized such crimes mainly into four types:

4. Crimes against individuals

Under this type, criminals usually target individuals to commit crimes, using technological equipment such as computers, mobile phones, etc¹⁰. There are multiple crimes against individuals, such as cyberstalking (an illegal practice wherein there is a use of any electronic area or medium to stalk others), slandering (an activity wherein criminals tend to tarnish a person's reputation by using the web as a platform for the same), phishing (acquiring the private information of persons by way of using laptops, cell phones, and other devices), etc.

5. Crimes against the government

All those crimes that are carried out against the legislature of any country or other administration come under crimes against the government¹¹. The major crime would be cyber terrorism. It refers to the use of any technological or online platform to enable the performance of harmful acts, politically or ideologically motivated. Often, such crimes may cause the loss of lives or properties.

6. Crimes against the society

When criminals engage in illegalities against numerous people at once, such crimes become crimes against society¹². It includes cyber trafficking (illegal buying and selling of humans over the Internet or other sites), cyber gambling (gamblers use mediums such as PCs or other online websites to interact with their fellow gamblers and get involved in betting activities), etc.

7. Crimes against the property

When we say crimes against property, it means illegal activities against such portable and elusive properties that come into creation through online platforms. A common type of crime

¹⁰ Shambhavi Tripathi, *Cyber Crime and Cyber Security : An overview*, IPLEADERS BLOG (Apr. 5, 2021, 9:50 PM) <https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/>

¹¹ Shambhavi Tripathi, *Cyber Crime and Cyber Security : An overview*, IPLEADERS BLOG (Apr. 5, 2021, 9:50 PM) <https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/>

¹² Shambhavi Tripathi, *Cyber Crime and Cyber Security : An overview*, IPLEADERS BLOG (Apr. 5, 2021, 9:50 PM) <https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/>

is cybersquatting, which refers to the registration, sale, or use of another person or company's intellectual property online and illegally profiting from their creation.

Laws governing privacy in cyberspace in India

Some laws in India seek to govern the arena of cyberspace, but what is necessary to understand is that they merely cover the subject matter relating to privacy. Currently, there is no legislation in the country dealing with it specifically. However, there have been attempts to bring the same into effect. Following is a brief providing information on all those laws and yet to be legislations:-

8. Constitution of India, 1949

As mentioned earlier, Article 21 of the Constitution also extends to an individual's privacy. It forms a part of a person's dignity and automatically comes under the purview of their life and personal liberty. In that sense, it becomes a fundamental right, and its infringement would call for the effect of relevant provisions of the nation's supreme law¹³. Also, because a person's private information is related to their privacy, the right to privacy includes data protection. But it would only be to the extent so far as the individual is entitled to that right.

9. Indian Contract Act, 1872

The Indian Contract Act, 1872 is the enactment that regulates all the contracts made within the territory of India. Clauses included in the agreements enforceable by law have to be subject to fulfillment by the concerned parties. In cases where there is a clause regarding data protection, parties must obligate by the same. If either of them causes any violations, the affected one may take up the matter in court. Accordingly, the legal consequences would flow from there.

10. Information Technology Act, 2000

In the 1990s, entered two of the most significant developments, globalization, and computerization, in India. There was an increasing use of computers and other such devices that continues to date. It ultimately led to the development of cyberspace. But with this creation, there was also a rise in the number of cybercrimes. To keep these crimes under control, the Government came up with the Information Technology Act, 2000. Apart from providing legal

¹³ Yashraj Bais and Raghav Vaid, *All you need to know about cyber laws in India*, IPLEADERS BLOG (Apr. 5, 2021, 9:29 PM), <https://blog.ipleaders.in/need-know-cyber-laws-india/>

recognition to all electronic transactions, it also provides provisions governing data protection. The Act seeks to prevent the breach of personal information and imposes penalties on criminals. An amendment in the year 2008 makes it more appropriate to deal with matters of privacy.

Section 43 of the Act calls for penalties for acquiring access to another person's computer or computer systems without their consent. It further provides compensation to the victim of such crimes. Section 66 deals with all the offences concerning computers. Section 66C states that any person impersonating someone else by stealing their private data will be liable to get punishment under this Act. Section 66D prohibits personation, and section 66E makes the invasion of privacy strictly illegal. Section 67 and its sub-sections take on sharing obscene material online. Section 72 imposes a penalty for infringement of confidential data. Section 72A deals with violations of privacy clauses in a lawful contract¹⁴.

11. Indian Penal Code, 1860

The Indian Penal Code, 1860 embodies statutory provisions for fraud, blackmailing, cheating, etc. These can also come into use for charging those who commit such crimes in cyberspace. But under this legislation, there can be no punishment against the criminal more than once. It is because it would violate their fundamental right under Article 20 of the Constitution.

12. Copyright Act, 1957

The Copyright Act, 1957 deals with all kinds of literary, artistic, and dramatic works coming under the purview of the digital arena. This legislation grants protection to intellectual property rights. If a person tries to imitate any of the works uploaded online, it would be equivalent to the breach of someone's copyright, and therefore, it would lead to penal consequences. The only thing that creates ambiguity here is what this Act considers to be data protection. Data protection means safeguarding the personal information of individuals, whereas this Act seeks to protect the creativity of the people.

Personal Data Protection Bill, 2019

As a result of the judgment delivered in the Puttaswamy case, a Committee of Experts came into existence in 2017. Justice B.N. Srikrishna was the chairman of the committee, and under

¹⁴ Yashraj Bais and Raghav Vaid, *All you need to know about cyber laws in India*, IPLEADERS BLOG (Apr. 5, 2021, 9:29 PM), <https://blog.ipleaders.in/need-know-cyber-laws-india/>

his supervision, it had to examine various issues of the protection of privacy. After a critical analysis, the committee drafted the Personal Data Protection Bill, 2017, which had a revision and was finally put forward before the legislature in 2019. Following are some of the significant provisions that the Bill provides:-

13. Application of the Bill

The Bill regulates the processing of the personal data of individuals by the governmental departments and the foreign companies that manage such data. It describes personal data as one through which a person becomes identifiable. The Bill also considers other types of personal information such as political beliefs, biometrics, etc., mainly because they are easily susceptible to cybercrimes.

14. Accountability of data fiduciary

The data fiduciary refers to an organization that makes decisions regarding the means and purpose of the data subject to processing by the government or other companies. There are certain limitations to such processing, meaning that the use of personal data can only be on lawful grounds. The data fiduciary, thus, mandatorily has to ensure the same. It has to come up with a security system that restricts the misuse of personal data. It also has to set up grievance mechanisms to hear people's troubles regarding their personal information and act on them. Finally, the data fiduciary has to implement a program of age-related verifications and parental consent to prevent the underage from accessing sensitive personal data¹⁵.

15. Data protection officer

Each data fiduciary must appoint for the post of a data protection officer a person who is well qualified and experienced. The main functions and responsibilities of data protection officers involve:

- The officer must maintain data records.
- They have to hold Data Protection Impact Assessments from time to time.
- They must act as a messenger or intermediary between the fiduciaries and the aggrieved.
- The officer has to make sure of compliance with the provisions of the Bill.

¹⁵ Beejal Ahuja, *Judicial interpretation of data protection and privacy in India*, IPLEADERS BLOG (Apr. 28, 2021, 12:50 PM), <https://blog.ipleaders.in/judicial-interpretation-of-data-protection-and-privacy-in-india/>.

16. Rights of individuals

There are a handful of rights that the Bill grants to individuals, which are as follows:-

- The right to inquire to the data fiduciary about whether the government or other companies processed their data.
- The right to rectify errors in their data or to update outdated information.
- The right to reveal their data before some other fiduciary in exceptional cases.
- The right to protect their data from leaking by the other fiduciary without their permission.

Grounds for processing personal data

The fiduciary can process the data only with the permission of its owner. But in certain situations, it would not be necessary for the fiduciary to obtain the owners' consent. If the processing is essential for the State to provide incentives to people, any legal proceedings, and medical emergencies, the fiduciary need not take prior permission from the owner¹⁶.

17. Offences

1. Any personal data processed without the owner's permission amounts to a violation of this Bill and would immediately invite a penalty of Rs.15 crores.
2. If the data fiduciary fails to protect the personal data, the Bill incorporates a punishment of the fiduciary by imposing a fine of Rs.5 crores.
3. Re-identification of any personal data would attract imprisonment of up to three years, or fine, or both.

18. Exemptions

The government can at any time exempt its agencies from the provisions of this Bill:-

1. if the security, public order, sovereignty, integrity, and the relations of the

¹⁶ Beejal Ahuja, *Judicial interpretation of data protection and privacy in India*, IPLEADERS BLOG (Apr. 28, 2021, 12:50 PM), <https://blog.ipleaders.in/judicial-interpretation-of-data-protection-and-privacy-in-india/>.

country with foreign countries are at stake.

2. If doing so prevents the incitement of a cognizable offence.

The processing of personal data is also exempt for:

1. Prevention and ill-treatment of an offence.
2. Journalistic or personal opinions.

19. Amendments to the IT Act

The Bill also aims at amending the IT Act, removing the provisions that call for payment of penalties by companies that fail to protect the personal data of individuals¹⁷.

Withdrawal of the the Personal Data Protection Bill

On 4th August 2022, the Central Government withdrew the Personal Data Protection Bill. It had been pending since its introduction in the Parliament. The Bill had been referred to the Parliamentary Standing Committee on Communication and Information Technology which prepared a report in December 2021 and submitted the same in Lok Sabha. The committee had proposed a long list of changes to the Bill, that is, 81 amendments and 12 recommendations¹⁸. Among other things, it suggested a single law that is aligned with contemporary privacy laws and the constantly evolving digital space. It also stated that the Bill must deal with both personal and non-personal data, and include provisions for the complete localization of data. The government, however, thought it would be better to come up with a new and better law instead of making several changes to the Bill. Also, various companies had concerns about the Bill demanding too much compliance.

Digital Personal Data Protection Bill, 2022

The Ministry of Electronic and Information Technology (MeitY)), on 18th November 2022, issued the draft Digital Personal Data Protection Bill. It has been kept open for public comment till 17th December 2022. The new Bill can be regarded as a condensed version of the earlier

¹⁷ Beejal Ahuja, *Judicial interpretation of data protection and privacy in India*, IPLEADERS BLOG (Nov. 28, 2022, 12:50 PM), <https://blog.ipleaders.in/judicial-interpretation-of-data-protection-and-privacy-in-india/>.

¹⁸ Ayushi Kar, *The withdrawal of PDP Bill and road ahead*, THE HINDU BUSINESS LINE (Nov. 28, 2022, 1:00 PM), <https://www.thehindubusinessline.com/blexplainer/the-withdrawal-of-the-pdp-bill-and-the-roadahead/article65747464.ece>.

bills. It restricts the proposed laws' scope to digital personal data protection. The aim is to lay down such dataprocessing norms that seek to strike a balance between an individual's rights in their data and the economic need to process the data for lawful purposes. Following are some of the significant features of the Bill:

20. Application and scope

The Bill applies to the following:

1. Digital personal data processing, subject to relevant exemptions (or material scope), and undertaken in India, and outside of India in certain cases.
2. Three key stakeholders in the cycle of data processing:
 - a. Data fiduciary (the person or entity deciding the purpose of processing an individual's data)
 - b. Significant data fiduciary (the person or entity dealing with a high volume of personal data)
 - c. Data processor (the person or entity who processes the data)
 - d. Data principal (the person whose data is being processed)

21. Consent and deemed consent

The Bill provides that the digital personal data of individuals must be processed for a lawful purpose and only with the consent of the data principal. The consent should be free, informed, and specific. It can also be withdrawn by the data principal at any point in time. The consequences of such withdrawal, however, have to be borne by the principal. The Bill also lays down the concept of deemed consent of the principal in certain situations, which range from compliance with the judgment or court order to public health crisis. But these situations are inclusive in nature.

22. Rights of individuals

Following are some of the major rights provided to individuals:

1. Individuals have the right to access basic information.

2. Individuals have the right to give their consent before their data is processed. They also have the right to withdraw their consent¹⁹.
3. Individuals have the right to nominate a person who can exercise these rights in the vent of their death or incapacity²⁰.
4. Individuals have the right to get the data collected by the data fiduciary erased and removed.

23. Cross-border data transfer

The Bill permits cross-border storage and transfer of data to countries and territories notified on this behalf. It is, however, subject to a suitable data protection landscape, from where the government can access the data of all Indians.

24. Exemptions

The Bill retains some exemptions from the previous bills and lays down some new ones as well.

1. The government can at any time exempt its agencies from the provisions of this Bill:
 - If the security, public order, sovereignty, integrity, and relations of the country with foreign countries are at stake.
 - If doing so prevents the incitement of a cognizable offence.
2. The government has the power to exempt certain businesses from complying with the provisions of the Bill. This exemption is based on the number of individuals and the volume of personal data that those businesses possess.

25. Establishment of the Data Protection Board of India

The Bill provides for the establishment of the Data Protection Board in the country in order to ensure compliance with its provisions. It also states that in case of any individual having a

¹⁹ *Digital Personal Data Protection Bill 2022*, DrishtiIAS, (Nov.28, 2022, 9:00 PM) <https://www.drishtias.com/dailyupdates/daily-news-analysis/digital-personal-data-protection-bill-2022>.

²⁰ *Digital Personal Data Protection Bill 2022*, DrishtiIAS, (Nov.28, 2022, 9:00 PM) <https://www.drishtias.com/dailyupdates/daily-news-analysis/digital-personal-data-protection-bill-2022>.

grievance related to the unsatisfactory response from the data fiduciary, they can file a complaint to the Board²¹.

Conclusion

The current data protection system of India is in dire need of some crucial improvements. There are a plethora of reasons for it. The provisions under the IT Act provide for the protection and processing of personal data by body corporate. There is no safeguard for other types of personal data that are freely available and accessible on many online platforms. For example, when the government links the Aadhaar to individuals' personal information, it will remain strictly intimate. The government will apportion it just with the Income Tax Department to give people beneficial services. But the operation of the department does not guarantee the privacy of personal information. It means that the Income Tax Act, 1961, governing the department does not incorporate any provision for the protection of personal data.

On the revelation of the Personal Data Protection Bill, many criticized it, stating that the government at any time can gain access to the private data of people on the grounds of sovereignty and public order. The Bill also sought to provide the government with unregulated powers to exempt its agencies from its regulations. Apart from that, in India, there's no age limit for creating accounts on social media platforms, where personal data is most vulnerable to breach.

The Personal Data Protection Bill had been retracted in August 2022 after the Parliamentary Standing Committee on Communication and Information Technology raised serious concerns about the effectiveness of the Bill once it became a law. The revised Digital Personal Data Protection Bill, issued in November 2022, seeks to balance out individual interests and public interests evenly. But the new Bill has already invited criticisms from civil rights and privacy activists. According to many, despite there being various called-for provisions (cross-border transfer of data), the Bill has been simplified to the extent of compromising individuals' protection. Moreover, it only deals with digitized personal data and provides no mention of non-personal data. There's no provision to notify the individuals about the breach of their privacy if it at all occurs. Also, it allows the government to access the personal data of users unconditionally, in the name of public or national interest. The latter has been given more

²¹ *Digital Personal Data Protection Bill 2022*, DrishtiIAS, (Nov.28, 2022, 9:00 PM) <https://www.drishtiiias.com/dailyupdates/daily-news-analysis/digital-personal-data-protection-bill-2022>.

importance than the former. Thus, much more is to be added to the Bill. It is still in the early stages and cannot be assessed properly at this point.