CHAPTER 5: CONCLUSION AND SUGGESTIONS

5.1 Conclusion

Technology Law is a new and growing field with a massive potential which will bring new opportunities and solutions on the table, like significantly reducing the cost and time of administration of justice, and the reduction in the justice gap.[1] A great example of this India is the “Tele-Law programme” by Department of Justice.[2] It is an effective and reliable e-interface and pre-litigation mechanism. It aims to connect needy and marginalized persons, in need of legal advice, through Para Legal Volunteers with Panel Lawyers via video conferencing/ telephonic facilities.

We started this journey by knowing how many internet users are here in India, and how many of those use a smartphone. The number of smartphone users and daily active internet users are increasing in India day by day. Every day, more and more people are using the internet, but the laws which are required to protect those internet users are lacking.

Through this paper, we understood the importance of the Right to Privacy, we understood how it is in danger, and how does the violation of the Right to Privacy is a human rights issue.

In Chapter 2 we also studied the evolution of privacy laws in India, and for this, we relied upon various court judgements. Then in the next chapter we understood how social media companies and Big Tech companies use our personal data for their profits, and we also studied the disadvantages of this current business model, where an individual's personal data is the raw material. At the end of Chapter 3, we explored various privacy respecting alternatives which we can use to claim our digital rights and protect our online privacy. We also learned how we can combat misinformation and fake news.

In Chapter 4 the researcher mentioned various laws related to right to privacy and technology around the world and in India. In this chapter, the researcher mainly covered the following countries; USA, Germany, United Kingdom, Spain, and India. The researcher also compared these laws and explained how governments in these countries intercept our personal communications. Through this, we learned the various legal mechanisms around the world and learned how they work.

In India a law was enacted called the Telegraph Act, 1885, this law regulated the procedure on how the government agencies can intercept the communications of the people, and how the agencies can tap their phone calls. The privacy implications which arose were dealt in People’s Union for Civil Liberties v. Union of India case.[3] In this case, the Supreme Court of India ruled that telephone tapping is a serious invasion upon an individual’s privacy. However, lawful interception can be carried out under certain circumstances

mentioned in the wiretapping provision. This kind of law interception has to be carried in conformity with certain guidelines, which will act as a check on indiscriminate wire-tapping by the law enforcement agencies. It also directed the government to make rules and procedures for carrying out lawful interception of communication. In addition to that, it also laid down the basic guidelines for such interception.

As per the procedure, a review committee is required to review the orders to intercept the communication of the people regularly. However, RTI reports show that this is generally not the case, and because the review committee is not doing their job properly, the privacy and liberty of the people are at risk. The lack of action by the review committee results is unregulated and unlawful actions by the authorities.

Then in the year 2000, the government enacted the Indian Information Act, 2000. Over the following years, the Act was amended with the current requirements of the time.

The Indian Information Technology Act, 2000 deals with the issues relating to payment of compensation (Civil) and punishment (Criminal) in case of wrongful disclosure and misuse of personal data and violation of contractual terms respecting personal data. This Act does have a provision to punish offenders who disclose private information, which is a good sign. However, there will be no data which can be leaked, if there is no data collected in the first place. In Chapter 4 the researcher highlighted the questionable and less than ethical business models of some Big Tech companies. These companies collect an enormous amount of data from their users, and they do this legally. The users of these services accept the terms and conditions and the privacy policy of their companies before using their services or products. Very few read those terms and conditions and the privacy policy before signing up for a service. Occasionally, the terms and conditions and the privacy policy are written in vague terms on purpose.

Last year when WhatsApp changed their terms and conditions and the privacy policy, many people questioned the change and raised their voices, many started to leave WhatsApp and started joining other messaging platforms.[4] Signal and Telegrams were the two apps which gained maximum amount of WhatsApp refugees. For Signal, the load on their servers were so much that their servers crashed for a day.

The exodus that took last year shows how much the current generation values their privacy and is willing to take steps to protect it. However, it was not enough because this mass shift only sent WhatsApp to its damage-control mode. WhatsApp postponed its policy update (so most people forgot about it again), and released a blog post explaining how user privacy is important to them. WhatsApp's users even saw a status message from WhatsApp of a banner explaining the users ‘how private and secure WhatsApp is’. WhatsApp also responded with advertisements in the local newspapers claiming that WhatsApp respects user privacy.

With this research, the researcher intend to understand few important topics as mentioned in the first chapter under the heading “Objective of the Study”. Over the duration of this entire research, the researcher was able to achieve those objectives. This research paper explains the meaning of right to privacy, studies the evolution of privacy laws in India, how companies exploit user data and how misinformation affects our society and lastly how to protect our digital rights.

5.2 Suggestions

Companies use vague terms all the time, which as a result confuses the public, and they are never questioned about it. Our laws are falling behind and are allowing big companies to exploit the public. Apart from vague terms in their terms and conditions and the privacy policy, companies also use dark patterns to confuse users and to exploit them. There is no law in India which regulate terms and conditions and the privacy policy of the companies, and which also ban the use of dark patterns. But first understand the vague language used in terms and conditions and the privacy policy of the companies, and for this let us take WhatsApp as an example.[5]

5.2.1 Does WhatsApp Protect And Secure Your Personal Messages? Let's Find Out.

1. We can't see your personal messages or hear your calls, and neither can Facebook: Neither WhatsApp nor Facebook can read your messages or hear your calls with your friends, family and co-workers on WhatsApp. Whatever you share, it stays between you. That's because your personal messages are protected by end-to-end encryption. We will never weaken this security, and we clearly label each chat, so you know our commitment.[6]

In theory, WhatsApp chats are end-to-end encrypted. WhatsApp, Facebook, or anyone in between, cannot read your messages. I say 'in theory' because there is no way of proving that. WhatsApp is a closed sourced proprietary software. A closed source software can be defined as a proprietary software distributed under a licensing agreement to authorised users with private modification, copying and republishing restrictions.

In simpler words, the source code is not shared with the public for anyone to look at or change. Closed source is the opposite of open source. Thanks, Wikipedia! So, we can't know what is going on behind the code. It is also quite likely that there is a backdoor in the WhatsApp source code, leaking all your sensitive data to governments, hackers, advertisers and the highest bidders.

Even with the encryption in place, and assuming that it's not a scam, WhatsApp regularly asks its users to make a security copy of their chats in the cloud, a copy that, by the way, is not encrypted and is indeed examined by, for example, Google Drive. So, like the Pompeii inhabitants, we are having our mistakes frozen and analysed forever.

This is why we should use an open sourced software.

2. We don't keep logs of who everyone is messaging or calling: While traditionally, mobile carriers and operators store this information, we believe that keeping these records for two billion users would be both a privacy and security risk, and we don't do it.

This is hard to believe. Isn't WhatsApp collecting 'metadata' (that too, unencrypted) on its users?

Metadata is data about your actual data.[7] It can be used to know a lot about you, like;

1. With whom you've been in contact, when and where.
2. When you are awake and when you go to sleep.
3. Which doctor you go to.
4. To whom you write a lot and to whom not at all.
5. When you are at work.
6. When you are sick and, when and where you go on a vacation.

From this type of data, WhatsApp/Facebook can create a profile about you, which they can sell to advertisers.

3. We can't see your shared location and neither can Facebook: When you share your location with someone on WhatsApp, your location is protected by end-to-end encryption, which means no one can see your location except the people you share it with.

That's true because everything you share is protected by end-to-end encryption. Nobody can read your messages except the recipient. This does not mean that WhatsApp or Facebook cannot collect your location data.

WhatsApp and Facebook cannot see your 'shared location'. But both of them can see your current location because it's as easy as looking at the signal of your mobile phone and finding out where it is coming from.

4. We don't share your contacts with Facebook: When you give us permission, we access only the phone numbers from your address book to make messaging fast and reliable, and we don't share your contacts lists with the other apps Facebook offers.

"WhatsApp does not share your contact lists with other apps Facebook offers," and
"WhatsApp does not share your contact lists with Facebook."

There is a difference between the two statements, a clear example of vague language to confuse people on purpose.

5. Groups remain private: We use group membership to deliver messages and to protect our service from spam and abuse. We don't share this data with Facebook for ads purposes. Again, these personal chats are end-to-end encrypted, so we can't see their content.

Groups remain private, really? A bug discovered on WhatsApp said otherwise. Over 400K, private WhatsApp group invite links are exposed to search engines.[8] Your WhatsApp groups may not be as secure as you think they are.[9]

5.2.2 Dark Patterns

Deceptive design patterns (also known as "dark patterns") are tricks used in websites and apps that make you do things that you didn't mean to, like buying or signing up for something. When you use websites and apps, you don't read every word on every page – you skim read and make assumptions. If a company wants to trick you into doing something, they can take advantage of this by making a page look like it is saying one thing when it is, in fact, saying another. You can defend yourself by learning about deceptive design.[10]

If you're an Instagram user, you may have recently seen a pop-up asking if you want the service to "use your app and website activity" to "provide a better ad experience." At the bottom, there are two boxes: In a slightly darker shade of black than the pop-up background, you can choose to "Make ads less personalized." A bright blue box urges users to "Make ads more personalized."

There's now a growing movement to ban dark patterns, and that may well lead to better, more thoughtful consumer protection laws and technology laws. It is important for India as well to keep their laws updated with time and new technology. Dark patterns have for years been tricking internet users into giving up their

data, money, and time. But if some advocates and regulators get their way, they may not be able to do that for much longer.[11]

Dark patters are defective by design, and yes, it is a design problem. The way software programmers or companies design their services or products can fall into any of the two categories. Good design and bad design. Dark patters are an example of bad design, they are intentionally designed to confuse users, or to make them do something without their knowledge. In contract law, there are few essentials elements which are required in an agreement to make it a valid contract. One of those essential elements is 'free consent'.

If the consent is not free, then the contract is void, as per the Indian Contract Act, 1872.[12]

Section 14: 'Free consent' defined. Consent is said to be free when it is not caused by:"

1. coercion.
2. undue influence.
3. fraud.
4. misrepresentation.
5. mistake.

Now, if we see the definition of fraud, as given in section 17 of the Act. As per section 17 (4) a fraud is any act fitted to deceive, and dark patterns are, in fact, deceiving people. Let us understand dark patterns with the help of some examples, and we will see if they are deceiving or not.

1. Confirmshaming

Confirmshaming is the act of guilting the user into opting in to something. The option to decline is worded in such a way as to shame the user into compliance. The most common use is to get a user to sign up for a mailing list, and it is often found in exit intent modals and other pop-ups. In the screenshot below, Google uses confirmshaming to discourage users from opting out.

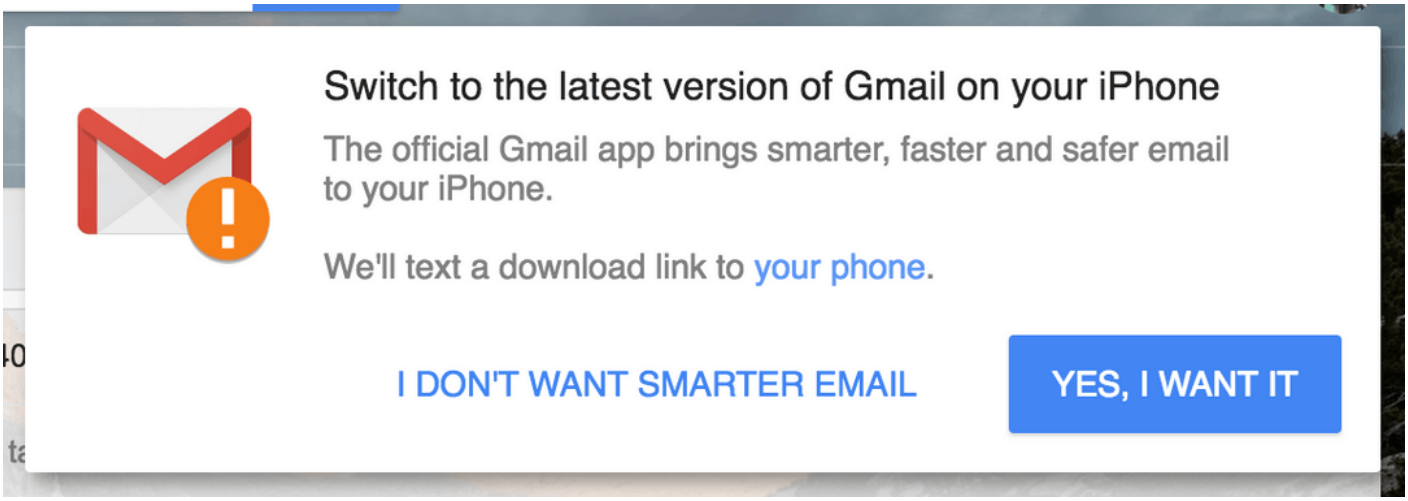

Fig 5.1: *An example of confirmshaming.*[13]

2. Disguised ads

Adverts that are disguised as other kinds of content or navigation, in order to get you to click on them. Softpedia is a popular software download site. One of their sources of revenue is display advertising. They often run advertisements that look like a download button, tricking users into clicking on the ads rather than getting the thing they wanted. In the screenshot below, the real download link is at the top left of the page. The disguised ads are highlighted in red.

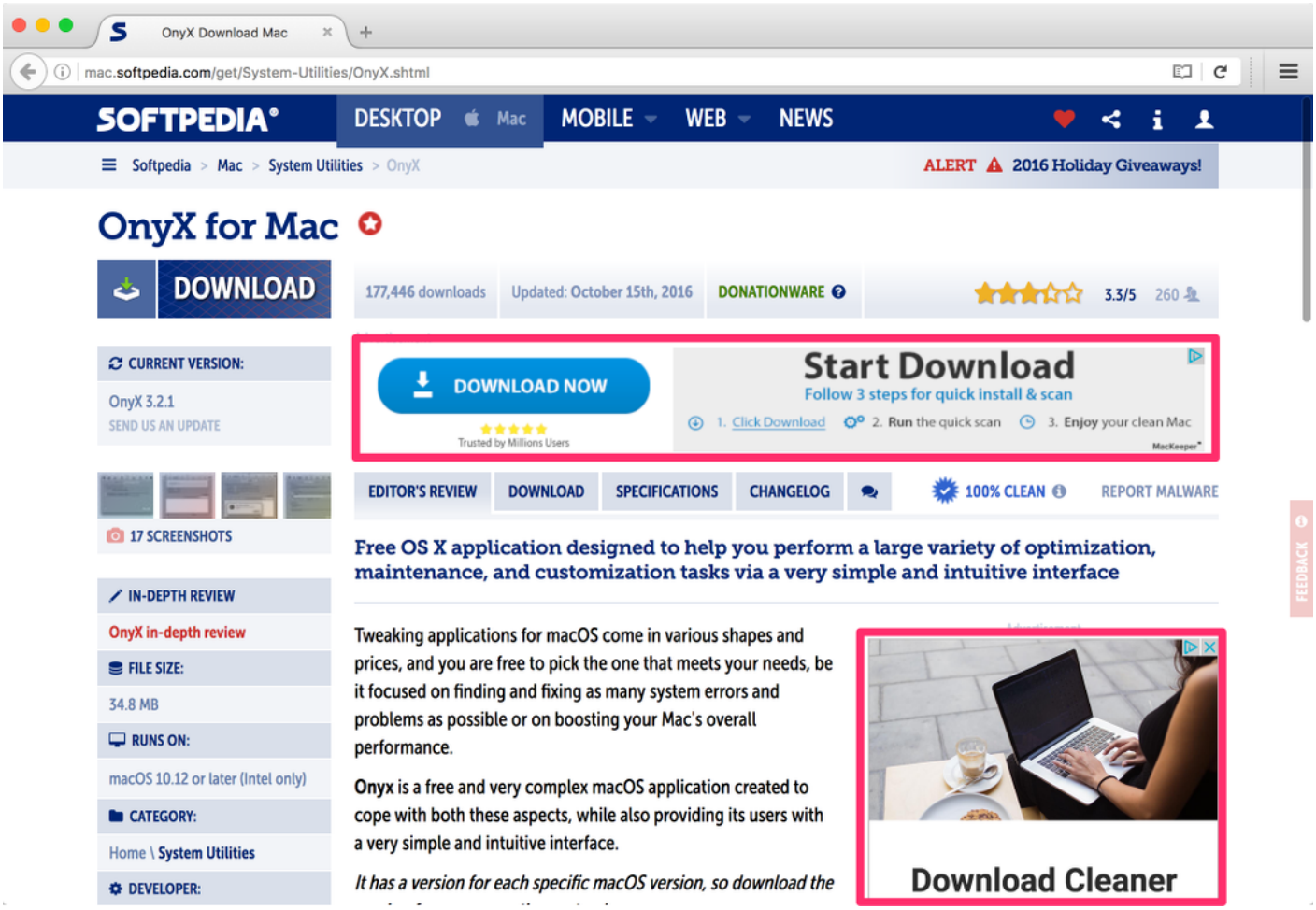

Fig 5.2: *An example of disguised ads.*[14]

3. Hidden terms

In this example, you can see a hidden checkbox.

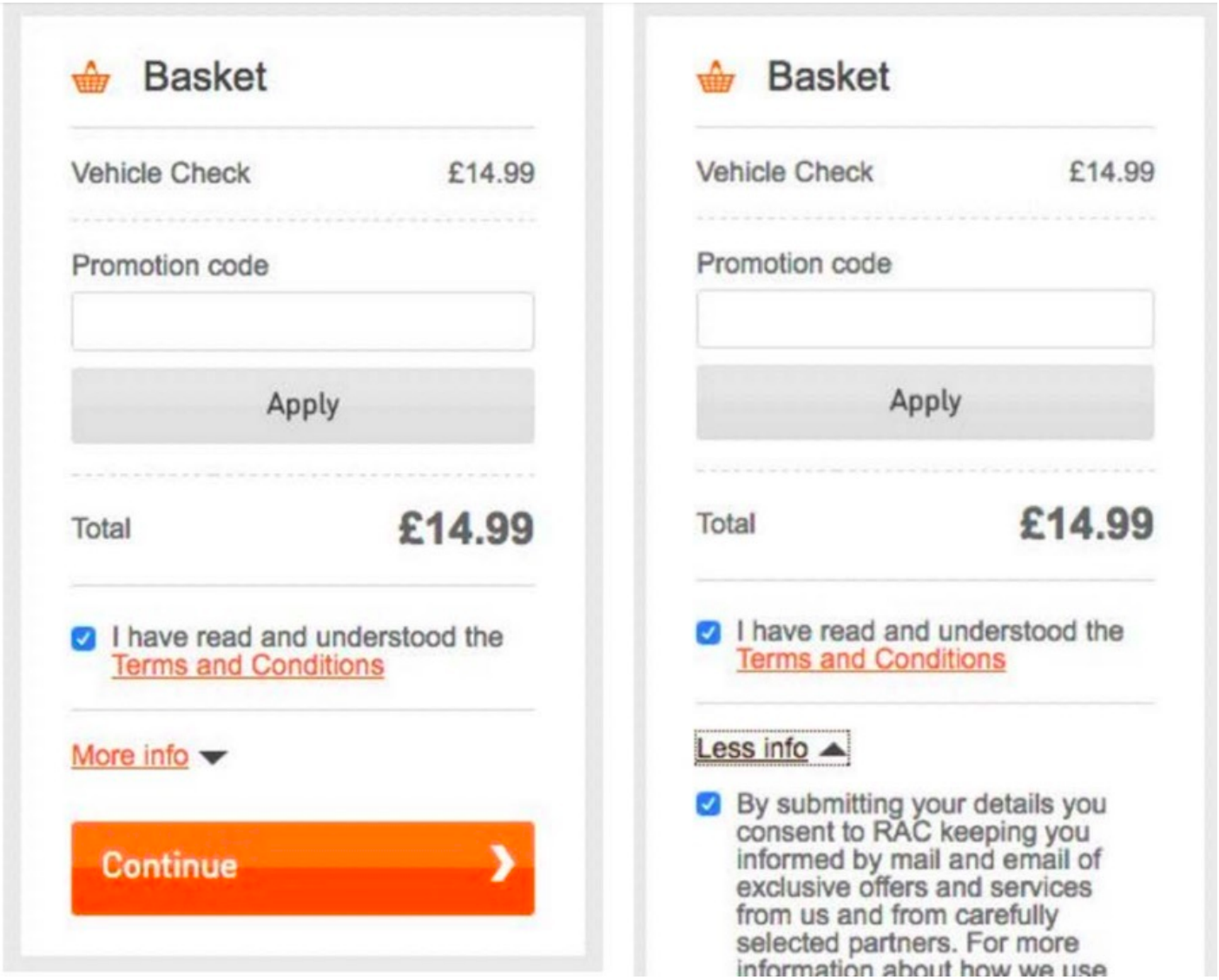

Fig 5.3: *Hidden check box.*[15]

There are many such example like these, and this type of design is used by almost everyone. Even WhatsApp did it to make more users agree to their new terms and conditions. But not all designs are defective. Some developers intentionally add light patterns[16], which are not designed to deceive anyone, in fact, they help the user to understand what is happening ad take control of the situation.

"You can also feel safe knowing we've built these subscriptions so that they only renew if you use Signal over the course of the month. Should you stop using Signal, or uninstall the app, they will be automatically cancelled after the next cycle, which helps eliminate the "dark pattern" of subscriptions you've forgotten about. We'll also be adding support for additional payment methods in the future."[17]

This extract is from a blog post published by Signal Foundation. Signal developers intentionally avoided dark patterns. Everyone should take a leaf out of Signal's book and implement 'white patterns' in their designs.

5.2.3 Data Removal

Under Europe's GDPR Law, a European citizen can request any company for data removal from their services or database. This provision of the GDPR puts the user back into the control of their data. This right is known as the right to erasure, it is defined in Article 17 of the GDPR.[18]

A similar provision is required in India. How many online accounts do you have? And how many of those services allow you to delete your accounts? The answer to the second question is, “not many”. There are many services don't even allow us to delete our accounts and the data stored on their servers. As mentioned above, Right to Erasure will empower Indians to take control of their data.

1. Deleting My Aadhaar

Any individual, irrespective of age and gender, who is a resident of India, may voluntarily enroll to obtain Aadhaar number. A person willing to enrol has to provide minimal demographic and biometric information during the enrolment process, which is totally free of cost.[19]

It is not mandatory to get an Aadhaar Card, though many people are unaware of this, and they thought getting an Aadhaar Card is mandatory. There can be many reasons for this misunderstanding, one can be illiteracy, or not knowing the full details before applying for an Aadhaar Card. What if someone who has an Aadhaar Card, wants the government to dele their data which they collected during the issuing of the Aadhaar Card? The same question was asked by Dr. Sanjay Singh and Shri Husain Dalwai in the Rajya Sabha in the year 2019.[20]

To which Shri S.S. Ahluwalia, on behalf of the Minister of State for Electronics and Information Technology, replied;

“Request for opting out of Aadhaar received. The UIDAI has not created a general option to exit from the Aadhaar Scheme. Pursuant to the judgement of the Hon’ble Supreme Court in Writ Petition No. 494 of 2012 Justice Puttaswamy (Retd) & Ans Vs UOI &Ors (26.9.18), such an exit scheme has only been mandated for children who have been enrolled with consent of their parents, who shall be given an option to exit on attaining the age of majority provided they do not intend to avail the benefits of the scheme (pg.556, majority judgement of Sikri J.). Accordingly, necessary steps to formulate such an exit scheme for children attaining majority is being created. No general option to exit from Aadhaar was laid down by the Hon’ble court as a binding direction, and consequently no such option has been created.”

Only children who were enrolled into the Aadhaar project with the consent of their parents have an option to exit from Aadhaar when they attain the age of majority. Having an option for adults to exit from Aadhaar also, will be a great option, which will empower the people to claim control over their data.

Under the Ayushman Bharat Digital Mission, people were issued a health ID called ABHA ID, a unique identity. The only problem was that it happened without the consent of the people who were issued these IDs. On the bright side, the government informed that the people will be able to opt out.[21] [22]

5.2.4 How to Claim Your Digital Rights?

1. Demand stronger data protection laws.
2. Read the terms and conditions before signing up for any service.

3. Be mindful of what social media platforms you use and how they use your data.
4. Limit the amount of data you share online.
5. Avoid using data hungry platforms altogether, and seek ethical alternatives.

Human Rights are interlinked, if one human right is violated, other human rights are also weakened. If one human right is protected, other human rights are also strengthened.

Similarly, if one person claims their digital rights, it helps others to protect and claim their digital rights as well. If one person gives up their digital rights, it weakens others' rights as well.

5.2.5 Artificial Limits

Another important aspect of modern technology, which is borderline unethical, is artificial limits. Artificial limits are not directed related to right to privacy, but it plays a considerable role in our society.

Have you ever tried to borrow an e-book from a library, and you found out that you cannot borrow it right now, as someone else have already borrowed it? It is a common thing, but the problem is, how can there be a shortage of a digital book? That is an example of artificial limits.

If you want to play an online video game on Xbox, you need the console, the video game, internet, and a subscription to play online. Why do we have to pay extra money to use the internet, which I already have?

Imagine a law which prohibits artificial limits in India. That law will change the Indian society. People might start reading more books because libraries don't have to put artificial limits, or people can freely use the internet they pay for, without any artificial limits.

The way we develop our technologies will impact the way our society evolves. It is important for us to consciously develop ethical, open, and people friendly technologies, to maintain a better, peaceful, and a democratic society.

Endnotes:

1Justice Gap is the gap between number of cases registered and the number of cases disposed off by the courts. Pendency of cases in the Judiciary increases the justice gap.

2Tele-Law: Reaching the Unreached. Department of Justice, Government of India. https://doj.gov.in/tele-law-scheme/ Last Visited on 24 May 2022.

3People's Union of Civil Liberties (PUCL) v. Union of India. Global Freedom of Expression. (2021, July 6). https://globalfreedomofexpression.columbia.edu/cases/peoples-union-of-civil-liberties-pucl-v-union-of-india/ Last Accessed on April 26, 2022.

4‘Hern, Alex’, “WhatsApp loses millions of users after terms update”, The Guardian (24 Jan 2021). https://www.theguardian.com/technology/2021/jan/24/whatsapp-loses-millions-of-users-after-terms-update Last Accessed on 11 May 2022.

5“The Privacy and Security of Your Personal Messaging”, WhatsApp. https://faq.whatsapp.com/general/security-and-privacy/answering-your-questions-about-whatsapps-privacy-policy?ref-banner Last Accessed on 11 May 2022.

6“WhatsApp’s Security”, WhatsApp. https://www.whatsapp.com/security/ Last Accessed on 11 May 2022.

7“What is Metadata?”, Harvard Law School. https://hls.harvard.edu/dept/its/what-is-metadata/ Last Accessed on 11 May 2022.

8‘Fedewa, J’, “Over 400K private WhatsApp group invite links are exposed to search engines”, XDA Developors (February 21, 2020). https://www.xda-developers.com/whatsapp-search-engine-group-invite-links/ Last Accessed on 11 May 2022.

9“WhatsApp Private Chat Groups EXPOSED on Google”, YouTube. (Jan 13, 2021). https://www.youtube.com/watch?v=od9QE7ZUIs0 Last Accessed on 11 May 2022.

10“Deceptive Design” https://www.deceptive.design/ Last Accessed on 11 May 2022.

11‘Morrison, S’, “Dark patterns, the tricks websites use to make you say yes, explained”, Vox. https://www.vox.com/recode/22351108/dark-patterns-ui-web-design-privacy April 1, 2021. Last Accessed on 11 May 2022.

12“Indian Contract Act, 1872”, Government of India.

13Confirmshaming - a type of deceptive design. Deceptive Design (formerly darkpatterns.org). https://www.deceptive.design/types/confirmshaming Last Accessed on 11 May 2022.

14Disguised ADS - a type of deceptive design. Deceptive Design (formerly darkpatterns.org). https://www.deceptive.design/types/disguised-ads Last Accessed on 11 May 2022.

15Davis, B. (2019, April 2). 13 examples of dark patterns in ecommerce checkouts. Econsultancy. from https://econsultancy.com/13-examples-of-dark-patterns-in-ecommerce-checkouts/ Last Accessed on 11 May 2022.

16Light Patterns: This term as been coined my the researcher. White patterns basically means the exact opposite of dark patterns. Design which is ethical, and is not intended to deceive the user.

17‘Moxie, M’, “Become a Signal Sustainer”. https://signal.org/blog/become-a-signal-sustainer/ (1 December 2021). Last Accessed on 11 May 2022.

18Article 17: Right to Erasure. ICO. https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-erasure/ Last Accessed on 12 May 2022.

19What is Aadhaar, Unique Identification Authority Of India, Government of India. https://uidai.gov.in/what-is-aadhaar.html Last Accessed on 12 May 2022.

20Option to Exit from Aadhaar, Unstarred Question No. 2652, Rajaya Sabha, Government of India. https://uidai.gov.in/images/rajyasabha/RSPQ_2652_(Unstarred).pdf Last Accessed on 12 May 2022.

21Ayushman Bharat Digital Mission: Creating India's Digital Health Ecosystem. ABHA number | ABDM. https://healthid.ndhm.gov.in/ Last Accessed on 12 May 2022.

22Health ID data privacy: Patients to be able to withdraw consent 'any time'. The Indian Express. (2020, August 26). https://indianexpress.com/article/india/centre-frames-draft-policy-on-data-privacy-under-national-digital-health-mission-6571123/ Last Accessed on 12 May 2022.

Revision #2
Created 6 November 2022 13:04:05 by ponytail
Updated 6 November 2022 13:11:23 by ponytail