

**Subject** : IGCSE Global Perspectives – 0457/02

**Component** : Individual Report (Component 2)

**Topic -Digital World**

## Global Research Question

**How do digital advertisements invade user  
privacy?**

---

### Candidate Details

**Candidate Name** - Aman Ladia

**Candidate Number** - 0051

**Centre No.** - IN405

**Exam Session** - May 2018

**Word Count** - 1968 exclusive of cover page, bibliography and footnotes

**Total no. of pages** - 12 (excluding cover page)

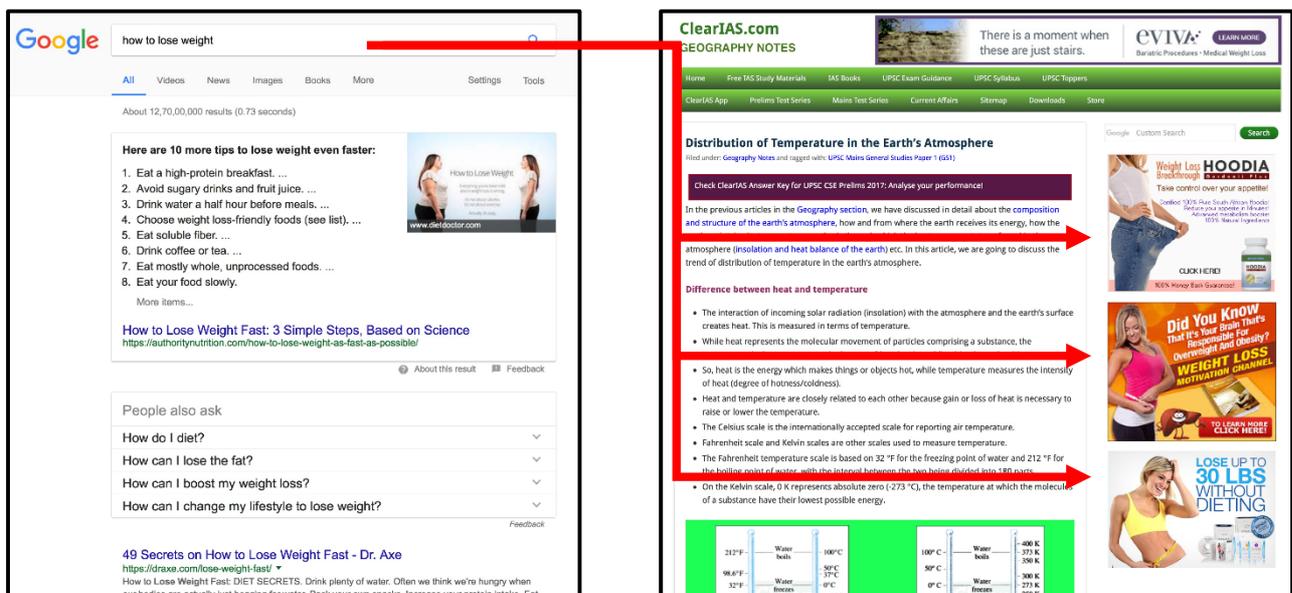
# How do digital advertisements invade user privacy?

## INTRODUCTION

Nearly 3.6 billion people<sup>1</sup> (46% of world's population) use the internet globally. What we fail to realise is that the business model of this supposedly 'free' service is based on collecting, analysing and selling user data for targeted advertising.

*'Targeted advertising is a form of advertising where online advertisers collect and analyse your data to target the most receptive audiences with certain traits, based on the product or person the advertiser is promoting'.*

This sounds convenient. But how is it that all website I visit these days—even educational ones—show me weight-loss ads(Pic.1)? Has Google been reading my search history? What else do they know about me? This report therefore aims to explore the implications of targeted advertising on people's privacy, and to evaluate the extent of this privacy invasion around the globe. The stance of different governments will also be assessed, including the perspective of my home country India, as 500 million Indians will be joining the internet within next decade under 'Digital-India project'.<sup>2</sup>



Picture-1 While I researched on how to loose weight, I was shown ads for weight loss all over a geography website

<sup>1</sup> Internet Users, accessed March 28, 2018, <http://www.internetlivestats.com/internet-users/>.

<sup>2</sup> "Digital India Programme," February 12, 2018, accessed March 28, 2018, <http://digitalindia.gov.in/>.

## KEY ISSUES

- Covert methods employed by advertisers to collect user-data without their conscious knowledge
- Harm inflicted by digital-advertisements on various levels of user-privacy
- Governments' stance and shortfalls of existing legislation for user-privacy

## GLOBAL PERSPECTIVE

Diagram-1 shows the different forms of data collected<sup>3</sup> by digital advertisers to predict which ads will interest a user the most. This ranges from non-personally identifiable information like your IP address, to sensitive personal data like emails, social security numbers, credit-card details, private photos etc. This has been obtained from Google, Yahoo and Facebook's advertising privacy policies, which are verified, reliable and up to date sources.<sup>4</sup>

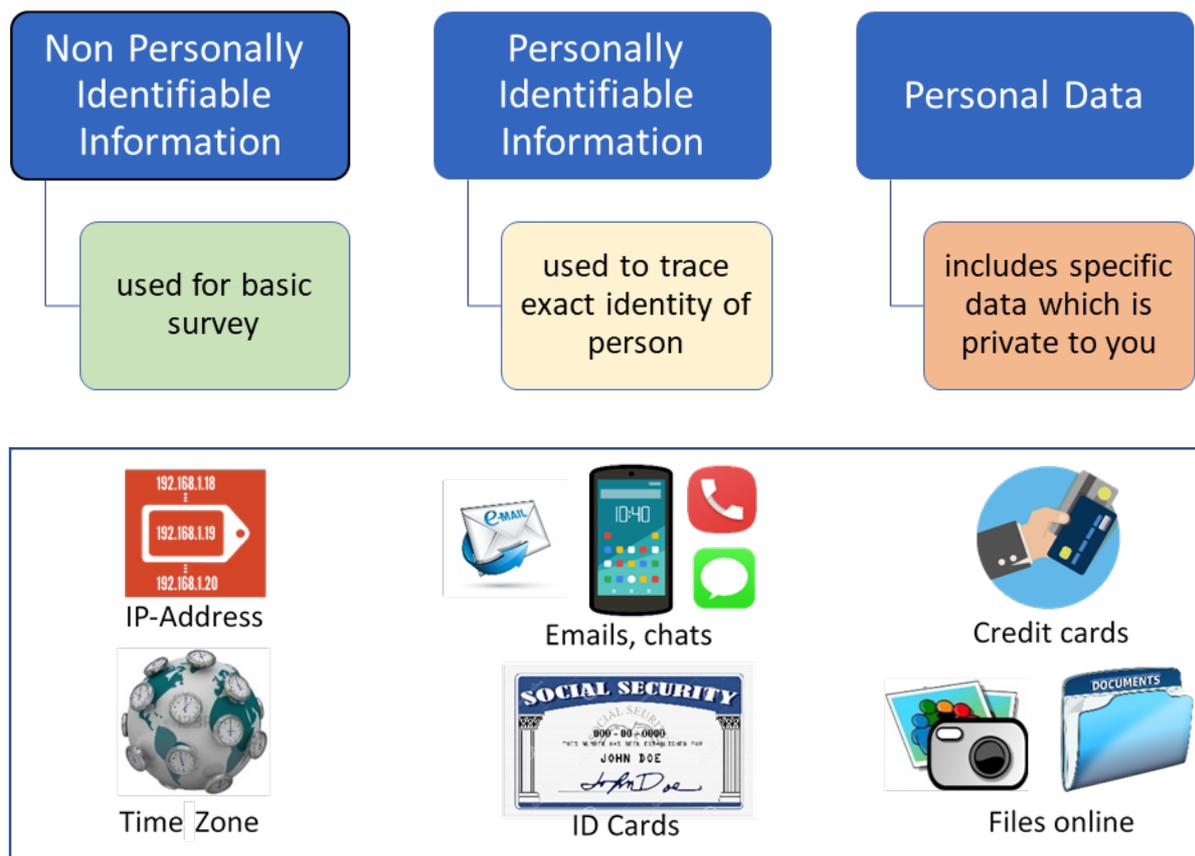


Diagram-1

<sup>3</sup> "Privacy Policy," Google, accessed March 28, 2018, <https://www.google.com/policies/privacy/?hl=en>.

<sup>4</sup> Google, Yahoo and Facebook receive most of their revenue from digital ads

While non-personally identifiable information is relatively benign as it is used for basic-survey only, the next category of collected data, i.e. personally identifiable information, poses a definite threat to the privacy of a user. Data regarding a person's browsing-history, phone-call logs, emails etc. is used to create highly targeted-advertisements<sup>5</sup>. A friend wrote an email to me about a new form of treatment for his concentration-disorder(ADHD), but soon after, he was left unnerved by ads from mental-clinics stalking him on every second page he visited. For me, this overpowers the convenience of options offered by ads.

Collection of 'personal-data', further deepens the potential of privacy-invasion in case of data leak/theft. It can lead to social embarrassment/stigma, when interests in taboo-topics or confidential issues become public by means of advertisements. In her personal testimony, Radha Deshmukh, a resident of Mumbai, blames Facebook for publicly revealing her 'like' on an advertisement for extra-large clothes (Pic-2), causing public embarrassment and ridicule. Lana Price<sup>6</sup> from the UK considers Facebook liable for the leak of her private photos through their ad platform, which nearly prompted her to suicide.



Picture-2

Further research suggests that using emails to transmit business documents/storing them on free cloud-services like Google or Yahoo Drive<sup>7</sup> can lead to disclosure of private-expenses as advertising programs go through personal documents stored online to extract information about socio-economic status. In fact, cybercriminals used digital-advertisements to find and redirect Italian-bank customers to fake-portals where their banking-passwords were compromised<sup>8</sup>. Identity-theft<sup>9</sup> has thus become much easier after the advent of digital-advertising.

<sup>5</sup> "Creepy Marketing Campaign," Marketing Hy, February 18, 2015, accessed March 28, 2018, <https://marketinghy.com/2015/02/call-stalking-call-amazing-marketing-create-creepy-marketing-campaign/>.

<sup>6</sup> Kara Gammell, The Telegraph, May-07, 2015, accessed March 28, 2018, <http://www.telegraph.co.uk/women/womens-life/11588667/Facebook-identity-theft-My-profile-was-stolen-to-get-dates-on-Tinder.html>.

<sup>7</sup> Yahoo! Accessed March 10, 2018 <https://policies.yahoo.com/us/en/yahoo/privacy/index.htm>.

<sup>8</sup> Intel, <https://securityintelligence.com/gootkit-malvertising-brings-redirection-attacks-to-italian-banks/>.

<sup>9</sup> Crime of obtaining the personal or financial information of another person to make fraud transactions

By invading user’s personal, social and financial privacy, it is therefore clear that digital-ads can infringe on a person’s privacy deeply(Diagram-2).

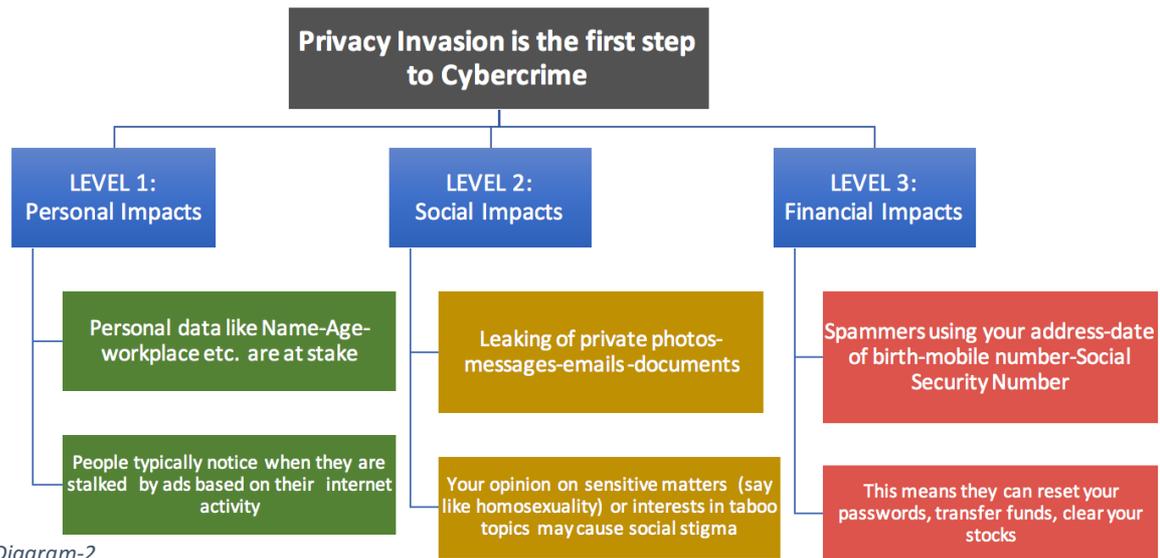


Diagram-2

Advertisers, however, transfer much of the blame of the social and financial repercussions of data collection to users. They argue that it is the user’s discretion to decide which private-files and photos to upload on the internet. Facebook, for instance, says that users should execute self-restrain by restricting the visibility of interests to ‘only me’ or ‘friends only’ to prevent unwanted data-collection. Nevertheless, the Digital Advertising Alliance—an association of e-advertisers—recently announced that emails will now no longer be read for data collection purposes. The alliance also decided to prohibit the use of race, religion, health and other sensitive details in targeted advertising.<sup>10</sup> These steps have received applause.

Advertisers also constantly state that they ask for user-consent before collecting data(pic-3).



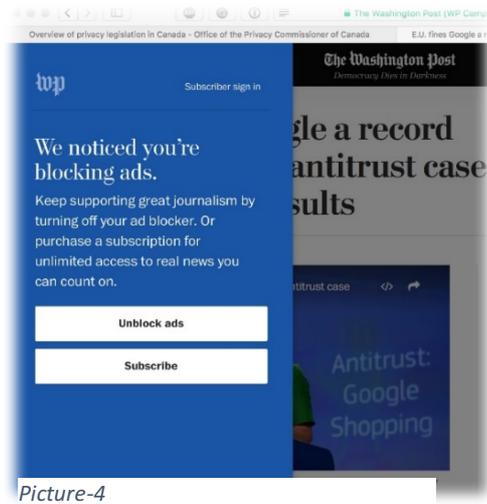
Picture-3

Google CEO Eric Schmidt says, “We know where you are, with your permission; we know where you’ve been, with your permission;”<sup>11</sup> Users can simply opt-out if they do not want data collection.

<sup>10</sup> "DAA News," March 14, 2018, accessed March 28, 2018, <http://digitaladvertisingalliance.org/daa-news>.

<sup>11</sup> "A Quote by Eric Schmidt," accessed March 28, 2018, <http://www.goodreads.com/quotes/792977>.

However, these arguments are only partially valid. The consent popup for data-collection(pic-3 above) of websites offers no real choice, consequently users are forced to click ‘agree’ to view the site. Furthermore, user discretion is hard to exercise when most people are unaware that even their private messages, photos and documents are monitored for advertising. Advertisers themselves admit that ‘scammers are reaching new heights’<sup>12</sup>, recognizing that the technology is fraud-prone. Acknowledging the threat of data misuse, websites like YouTube and Washington Post(pic.4) are now offering paid ad-free subscriptions for the privacy-conscious.



Picture-4

As I tried to understand the extent of invasion in various countries, I first collected primary data by interviewing Mr. Puneet Gupta, a cyber-security specialist working at Security Research Labs<sup>13</sup>, who claimed-

*“People living in developed countries suffer from a significantly higher risk of identity-theft as advertisers earn significantly more from developed countries than from developing ones”.*

**Digital Ad Revenue (2016)<sup>14</sup> vs Identity Theft<sup>15</sup>**

Country	Digital Ad-Revenue	Identity-Theft(~Bn\$)
United States	\$82bn	16
EU Combined	\$45bn	12
China	\$30bn	9
Kenya	\$0.3bn	0.07

Table-1

<sup>12</sup> Lucian Constantin, Computerworld, May 15, 2014, accessed March 28, 2018, <https://www.computerworld.com/article/2489436/security0/online-advertising-endangers-user-security-privacy.html>.

<sup>13</sup> "Security Research Labs-GmbH," accessed March 18, 2018, <https://srlabs.de/>.

<sup>14</sup> "Statista Market Forecast," accessed March 22, 2018, <https://www.statista.com/outlook/216/102/digital-advertising/> [Verified Statistics aggregator]

<sup>15</sup> "Global Fraud Report.jpeg," accessed March 28, 2018, <https://goo.gl/zgpyr3>.

Both table-1 and Mr. Gupta's expert testimony confirm our claim that markets where digital-advertisers are most active also suffer from the maximum identity theft. But why is it that China has significantly lower identity theft even though its economy is comparable to USA? A Reuters report<sup>16</sup> suggests that the US-Government relies on data collection by ad-agencies for national/international intelligence. Subsequently, US' varying data-protection laws from industry-to-industry help advertisement giants dodge legal action. China has virtually banned Facebook and Google<sup>17</sup>, as it considers digital-ads a threat to national security. Despite vested interests, both the countries clearly acknowledge that digital ads indeed invade user privacy.

To counter this, EU has taken a moderate yet effective stance in favour of users. It recently fined Facebook \$122 million for unauthorized exchange of private-data<sup>18</sup> and ordered them to delete all past data-records. The European 'Digital-Single-Market' plan<sup>19</sup> by default ensures advertisements will not collect user-data unless the user explicitly changes the setting to 'opt-in'. This is a big win as it provides a uniform privacy safety cover to 28 countries in EU. Digital ad-revenue is likely to experience a fall in EU after its implementation but this should get offset by decline in print-media as ad becomes more digital.

This leads to the question-what beyond EU boundaries? Digital-advertisers work on global platform. Hence world requires regularisation of data collected by ads through an international organisation like the UNHRC<sup>20</sup> to safeguard global Internet-users. As opposition against digital advertising increases through the growth in ad-blocking software,<sup>21</sup> self-restraint by advertisers is must to ensure a mutually beneficial relationship for both consumers and websites.

---

<sup>16</sup>Joseph Menn, Reuters, October 05, 2016, accessed February 15, 2018, <http://www.reuters.com/article/us-yahoo-nsa-exclusive/exclusive-yahoo-secretly-scanned-customer-emails-for-u-s-intelligence-source-idUSKCN1241YT>.

<sup>17</sup>"Pinterest," CNNMoney, accessed March 28, 2018, <http://money.cnn.com/gallery/technology/2016/05/23/banned-china-10/6.html>.

<sup>18</sup>Mark Scott, "E.U. Fines Facebook \$122 Million," The New York Times, May 18, 2017, accessed February 15, 2018, <https://www.nytimes.com/2017/05/18/technology/facebook-european-union-fine-whatsapp.html>.

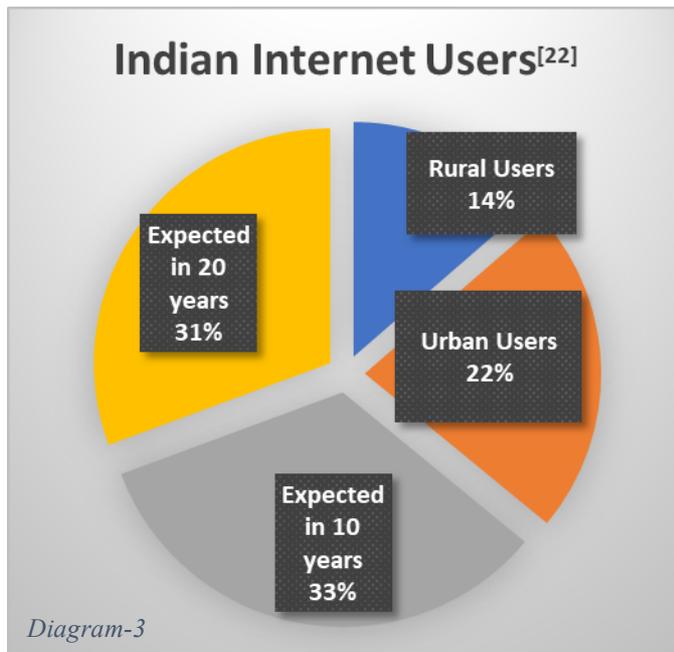
<sup>19</sup>Digital Single Market, accessed March 14, 2018, <https://ec.europa.eu/digital-single-market/en/taxonomy/term/75985>.

<sup>20</sup>United Nations Human Rights Council

<sup>21</sup>Software that removes advertisements from websites:<https://pagefair.com/blog/2017/adblockreport/>

## National Perspective

India, a newly industrialized country, is experiencing rapid growth in the technology sector. Indian internet users have grown from 5 million in the year 2000 to nearly 460 million in 2016<sup>22</sup>, a huge market potential for digital-advertisers.



This graph (from a verified government-report) indicates around 36% of the Indian population currently uses the internet(Diag.3). When I asked my house-help about what she felt about privacy, she said [*translated*]:

*“In my village, everybody is illiterate. They cannot even sign their name. They put their thumb print wherever they are asked, without reading what it’s for.”*

For 163mn<sup>22</sup> rural users, privacy is least of their problems (leave alone digital-privacy). The 269 million urban users<sup>22</sup> on other hand have just started to enjoy the internet-boom. The lack of education and awareness makes Indians more liable to privacy invasion by digital-ads. Some friends and family members that I personally interviewed said that ads offer a great shopping experience by providing more options and publicizing discounts, but were extremely ignorant about data-theft related impacts. However, when I discussed social impacts(Diag.2) like public exposure of private interests, they were alarmed. In the traditional, sensitive Indian society, the social impacts of data-collection have a much greater impact that in the western world.

On August 25, 2017, The Supreme Court of India finally recognized the fight to strengthen privacy-laws, and ruled that “Privacy is a fundamental right, an integral part to the right to

<sup>22</sup> Internet in India, report, Internet and Mobile Association of India, <http://bestmediainfo.com/wp-content/uploads/2017/03/Internet-in-India-2016.pdf>.

life as guaranteed by Constitution of India”<sup>23</sup>. This verdict potentially arms citizens with the right to question how websites use and share user data. ‘Fraud Report 2016’ by Experian India<sup>24</sup> suggests that identity-theft accounted for 77% of financial frauds in year-2015 in India. But despite privacy as a fundamental right, cases against advertisers (like WhatsApp and Facebook) for breach of user-privacy cannot be reopened until “a robust regime for data protection laws are put in place”<sup>25</sup> by the government.

My research concluded that Indians are trapped in a Sphere of Privacy Invasion, as depicted below:

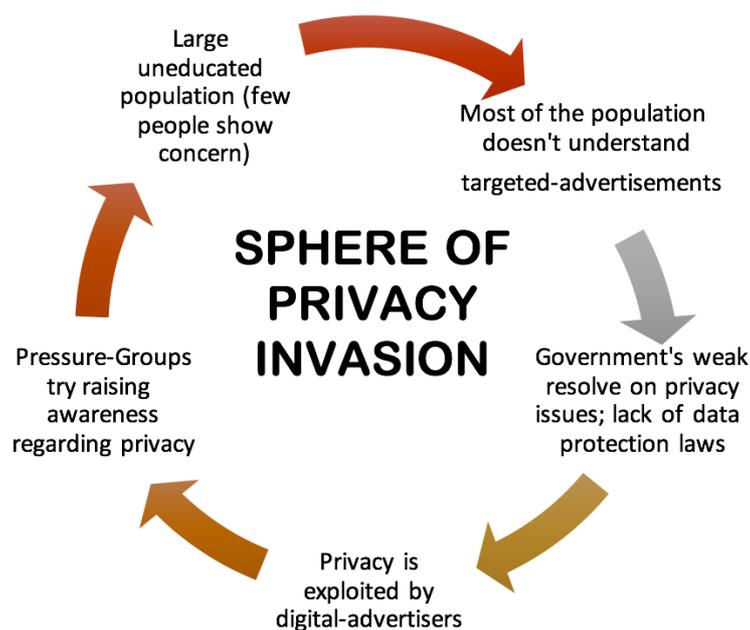


Diagram-4

This cycle is set to become increasingly threatening as nearly 500 million Indians join the internet within next decade due to the Government’s ‘Digital-India’ project<sup>26</sup>. Being largely digitally illiterate, new users are more vulnerable to privacy-invasion. A bigger worry is that many Indian companies are entering the digital ad-market without sufficient security measures; if they are not made accountable, Indians will stand exposed to data-thefts.

<sup>23</sup> "Judgment of Chief Justice," Scribd, accessed February 05, 2018, <https://www.scribd.com/document/357101536/Judgment-of-Chief-Justice-J-S-Khehar-and-Justices-R-K-Agrawal-S-Abdul-Nazeer-and-D-Y-Chandrachud>.

<sup>24</sup> <http://www.experian.in/assets/Experian-launches-India-Fraud-Report-2016.pdf>

<sup>25</sup> "Judgment of Chief Justice," Scribd, accessed February 05, 2018.

<sup>26</sup> "Digital India Programme," February 12, 2018, accessed March 28, 2018, <http://digitalindia.gov.in/>.

The government's stance is that the right to privacy is "*not absolute*"<sup>27</sup>, and that '*needs of India's digital-industry which has potential to become a trillion-dollar economy has to be addressed as well*'<sup>28</sup>. Digital-ads generate more than 1 billion dollars/year<sup>29</sup> for India. Striking a compromise between revenue and privacy is difficult but rising identity-thefts<sup>30</sup> will soon exceed the ad-revenue. Nevertheless, the government has finally agreed to work on a feasible data protection act,<sup>31</sup> a whitepaper of which was released in December-2017.<sup>32</sup> Consequently, major advertisers have issued written commitments that that steps are being taken to prevent data-misuse.<sup>33</sup>

Hence, what India requires hereafter is a large-scale 'National-Digital-Literacy-Mission' to break this 'Privacy Invasion-Sphere'; although India's huge population poses obstruction to its quick implementation. NGOs<sup>34</sup> and media-outlets should simultaneously continue to build pressure to ensure that a comprehensive data-protection law is implemented by Government quickly.

## **Personal Reflection**

As an avid internet user, I have seen the advertising consent popup on many webpages, but I always believed that the kind of data collected by them was restricted to basic personal information. The social and financial risks associated were somewhat unknown to me. I still admit that advertisements are useful, and even desirable at times. I also concede to the fact that advertising is necessary to keep the internet free. But what concerns me is that accountability of advertisers towards user's data is amiss due to lack of comprehensive

---

<sup>27</sup> "Privacy a Fundamental Right," The Times of India, August 24, 2017, accessed February 05, 2018, <http://timesofindia.indiatimes.com/india/privacy-a-fundamental-right-subject-to-reasonable-restrictions-government/articleshow/60208427.cms>.

<sup>28</sup> Roadmap for US\$1 Trillion Digital Economy, accessed February 04, 2018, <http://pib.nic.in/newsite/PrintRelease.aspx?relid=165697>.

<sup>29</sup> Statista, accessed February 7, 2018, <https://www.statista.com/statistics/233468/advertising-revenue-in-india-from-2011/>.

<sup>30</sup> <http://www.experian.in/assets/Experian-launches-India-Fraud-Report-2016.pdf>

<sup>31</sup> "Data Protection Bill," August 26, 2017, accessed March 22, 2018, <http://economictimes.indiatimes.com/news/economy/policy/data-protection-bill-to-be-in-place-by-december-law-minister-ravi-shankar-prasad/articleshow/60227629.cms>.

<sup>32</sup> White Paper on Data Protection, accessed March 19, 2018, <http://meity.gov.in/white-paper-data-protection-framework-india-public-comments-invited>.

<sup>33</sup> <http://trak.in/tags/business/2018/03/23/facebook-wont-be-misused-during-indian-elections/>

<sup>34</sup> Digital Citizens and Their Rights in India, accessed March 22, 2018, <https://www.apc.org/en/blog/digital-citizens-and-their-rights-india>.

legislation and Governments' vested interests. At the same time, the lack of awareness even amongst educated people in my country about how their e-activities provide advertisers free access to their private information reinforces the necessity of grass root campaigns at school and college levels.

As an individual, I tried using Virtual Private Networks (VPN), Ad-Blocker software, Proxies, and paid subscriptions to protect my privacy. While they did help me to some extent, I was frequently locked out of many websites, forcing me to disable these services from time to time.

My opinion on paid-websites has changed after researching this topic: at least they give you an option to protect your privacy. Paid-internet has a scope for further research. The stance of the EU impacted me the most: human rights supersede tax revenue. The recent declaration of privacy as fundamental right in my country is now pushing advertisers like Facebook and Google towards taking measures to safeguard personal data and making the experience more transparent.<sup>35</sup>

Accordingly, a tri-partisan action is needed: if advertisers exercise self-restraint in intrusive advertising by not taking privacy for granted, users understand their e-activities and a global legislation is established with respect to data protection laws, only then can a Radha in India, Lana in UK and the 3.6 billion internet users *safely enjoy free internet all over the globe*. The extent of privacy invasion may be different for each of us, but we all suffer from the same ethical, social and material implications of intrusive data collection.

---

<sup>35</sup>"Facebooks New Identity Theft Prevention Features," FactorDaily, accessed March 11, 2018, <https://factordaily.com/news/facebook-india-profile-picture-guard-design-identity-theft/>.

## Bibliography

### Books

Richards, Neil. *Intellectual privacy: rethinking civil liberties in the digital age*. Oxford, UK: Oxford University Press, 2015. n.d.

Acquisti, Alessandro. *Digital privacy: theory, technologies, and practices*. Boca Raton, FL: Auerbach, 2008. n.d.

Mills, Jon L. "Privacy and Its Contemporary Context: Why Privacy Is Disappearing." *Privacy*, 2008, 13-104. doi:10.1093/acprof:oso/9780195367355.003.0003. n.d.

### Magazine Articles

Stone, Jeff. "Digital Privacy Campaign Urges Users to Dump Yahoo." *The Christian Science Monitor*, October 13, 2016. n.d.

Milne, George R. *Digital privacy in the marketplace: perspectives on the information exchange*. New York, New York (222 East 46th Street, New York, NY 10017): Business Expert Press, 2015. n.d.

### Reports

Google. 2016. *Google Transparency Report*. December 31. Accessed April 22, 2017. <https://www.google.com/transparencyreport/userdatarequests/countries/>.

Internet and Mobile Association of India. 2016. *Internet in India: 2016*. Accessed July 17, 2017. <http://bestmediainfo.com/wp-content/uploads/2017/03/Internet-in-India-2016.pdf>.

Sussman, Heather Egan Hine, Carla A. R. Panich, and Evan D. "Privacy and Data Protection: 2012 Year in Review." *Mondaq Business Briefing*, January 29, 2013. Accessed July 17, 2017. [http://www.highbeam.com/doc/1G1-316790880.html?refid=easy\\_hf](http://www.highbeam.com/doc/1G1-316790880.html?refid=easy_hf). n.d.

### Website Articles

Bedy, Rudy Gabriel. n.d. *Marketing Repository*. Accessed 4 22, 2017. <http://www.rudibedy.com/blog/facebook-advertising-cpc-cpm-per-country/>.

Butler, Brandon. 2013. *4 Internet privacy laws you should know about*. March 12. Accessed April 22, 2017. <http://www.networkworld.com/article/2164315/lan-wan/4-internet-privacy-laws-you-should-know-about.html>.

- Gammell, Kara. 2015. *My Facebook profile was stolen to get dates on Tinder - and there's nothing I can do*. May 07. Accessed April 23, 2017. <http://www.telegraph.co.uk/women/womens-life/11588667/Facebook-identity-theft-My-profile-was-stolen-to-get-dates-on-Tinder.html> .
- Goel, Vindu. 2016. *Yahoo Says 1 Billion User Accounts Were Hacked*. December 14. Accessed April 22, 2017. [https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?action=Click&contentCollection=BreakingNews&contentID=64651831&pgtype=Homepage&\\_r=1](https://www.nytimes.com/2016/12/14/technology/yahoo-hack.html?action=Click&contentCollection=BreakingNews&contentID=64651831&pgtype=Homepage&_r=1).
- Kenneth Olmstead, Aaron Smith. 2017. *What the Public Knows About Cybersecurity*. March 22. Accessed April 22, 2017. <http://www.pewinternet.org/2017/03/22/what-the-public-knows-about-cybersecurity/>.
- Korolova, Aleksandra. 2011. 11 13. Accessed April 22, 2017. [https://theory.stanford.edu/~korolova/Privacy\\_violations\\_using\\_microtargeted\\_ads.pdf](https://theory.stanford.edu/~korolova/Privacy_violations_using_microtargeted_ads.pdf).
- Loras, Sophie. 18. July 2016. Accessed April 2017, 22. <https://www.clickz.com/what-do-chinas-new-online-advertising-rules-mean-for-marketers/103221/>.
- Monyango, Francis. 2016. April 1. Accessed April 22, 2017. <http://www.nairobibusinessmonthly.com/politics/consumer-privacy-and-data-protection-in-e-commerce-in-kenya/>.
- Sullivan, Danny. 2012. March 9. Accessed April 22, 2017. <http://marketingland.com/pew-survey-targeted-ads-negatively-7548>.