International Journal of Advanced Educational Research
ISSN: 2455-6157
Impact Factor: RJIF 5. 12
www.educationjournal.org
Volume 2; Issue 5; September 2017; Page No. 25-29

A click on I Agree? We've all done it: Clicked or Skipped

[1] Nakul Sharma, [2] Rahul Vyas
[1] 2nd Year LL.B. Student, Pacific School of Law, PAHER University, Udaipur, Rajasthan, India
[2] Assistant Professor, Pacific School of Law, PAHER University, Udaipur, Rajasthan, India

Abstract
Today's verdict by The Supreme Court 9 judges bench declared that the right to privacy is protected under Article 21 & Part 3 and is a Funadamental Right in an unanimous. The Apex court pronouncements in a plethora of cases Malak (1981), Rajagopal (1994), Selvi (2010), Nalsa (2014) have all made a point clear as to privacy as a constitutional part 3 right, as What we upload over internet or social media, cloud backups, must only be shared with the people we want to and they should not be misused to manipulate the minds of shoppers especially. What we upload should strictly be not used to identify us & sold to third-parties by such companies whom we trust and give our data to keep safe. Many people store their banking details, passwords, documents over the cloud storage or emails to get the easy access.
The tectonic shifts in Technology and advent of Algo's, AI, ML and Robotics have made a sea of difference in the strategy for business. E commerce is being used for sale and purchase of several products and services using diverse portals and websites. The more the internet services are being used the more are we getting our privacy in fringed?
To Agree with the terms and conditions of the company which are inscribed to get what companies wants. By this time, we've grown confident enough that there's probably nothing wrong in that fine pact or standard form of contract that is worth wasting time for.
But once in a while companies put needle in the straw, something that we just not bargained for.
When we all use or install apps, we click on "I Agree", "I Do Not Agree" or "I Accept" most of the time to use the service we accept. The present paper is a commentary on the various facets of the Information Technology Laws and how its implementation is taking place globally.

Keywords: agree, technology, globally, banking

Introduction: What you are really agreeing huge agreements for?

Uber Cabs

The cosmic terms are mostly useless for the users, Oftentimes they are: You have to be 18 years old or greater to use Uber services; Don't use stolen debit/credit cards for payments, pricing, etc.
Importantly: Uber is terms about the responsibility towards drivers & their services.
"[UBER] will not be a party to disputes, negotiations of disputes between you and [cab drivers].
In short use it at your own risk; uber is not responsible for if someone is kidnapped or raped while using uber cabs.

Airtel

Many people now days are using airtel app in smartphones to keep track of data use, to check on bills / to recharge, now days airtel has also launched Payments Bank.
Privacy Policy: Airtel explained in the section "Collection of Personal Information: that airtel or its employees may utilise some or all available personal information for internal assessments, measures, operations, and related activities."

Importantly

"We may transfer your personal information or other information collected, stored, processed by us to any other entity or organisation located in India or outside".
Airtel obtains consent from the customers by leading them to click on I ACCEPT.

Paytm

Paytm is well known for its e-wallet services and soon planning to be a bank. We share our debit/credit cards, DOB, Sex, For KYC Aadhaar and Pan details now days.
Terms and Conditions: In Links to other sites section is says
"Our site links to other websites that may collect personally identifiable information about you. Paytm is not responsible for the privacy practices or the content of those linked websites".

True caller

Most widely used app these days in India. By accepting to its terms we are allowing not only our privacy being compromised but of others as well.

Privacy Policy

"By accepting the true caller privacy policy and/or using the services you consent to the collection, use, sharing and processing of personal information."
"if you provide us with personal information about someone

else, you confirm that they are aware that you have provided their information and that they consent to our use of their information according to our privacy policy".
Not only this but True caller shares our personal information and location.
"We may use any of the information collected, as set out above, to provide you with location and interest based advertising, marketing messaging, information and services. We may also use the collected information to measure the performance of our advertising and marketing services".
True caller also transfer information to vendors, service providers.
"True caller may also share personal information with third party advertisers, agencies, and networks."
Now you know the source of all the marketing calls you have been getting these days on your mobile phones.

Instagram
A great source of marketing companies and sellers to reach their customers but at what cost?

Terms and Conditions
"Instagram, its affiliates, or service providers may transfer information that we collect about you, personal information across borders and from country or jurisdiction to other countries or jurisdictions around the world"
"Please note that we may transfer information, including personal information, to a country and jurisdiction that does not have same data protection laws as your jurisdiction"
"We may also share certain information such as cookie data with third-party advertising partners. This information would allow third-party ad networks to, among other things, deliver targeted advertisements that they believe will be of most interest to you".

Facebook
Widely used and popular social networking service.
Have you ever felt that what you searched on your browser to buy suddenly pops up in advertisements while scrolling down your Facebook feed? Or;
The company advertisement to sell mobile cover of the very same model you surprisingly use?
Terms of Service:
"When you use an application, the application may ask for your permission to access your content and information as well as content and information that others shared with you".
"We want out advertising to be as relevant and interesting as the other information you find on our services. With this in mind, we use all of the information we have about you to show you relevant ads".
"We transfer information to vendors, service providers, and other partners who globally support our business".
Ipr infringements rights that we give consent to;
"for consent that is covered by intellectual property rights, like photos and videos (ip content), you specifically give us the following permission – you grant us a non-exclusive, transferable, sub-licensable, royalty free, worldwide license to use any ip content that you post on or in connection with facebook (ip license)".

What is Privacy Protection & Data Security?
Everyone has the right to privacy, currently it is a big fat question for the Supreme Court of India whether such privacy is a Fundamental Right to the citizens of India?
People have right to secrecy for the personal data concerning them, that they store or share online and especially with regard to their private and family life.
Cyber-crimes are the risk to data security, cyberspace is a complex environment consisting of interactions between people, software and services supported by worldwide distribution of Information and Communication Technology (ICT) devices and networks. Cyberspace is the common pool used by citizens, businesses, critical information infrastructure, military, government in a manner that makes it difficult to draw clear boundaries.
Cyberspace is expected to be more complex foreseeable future, with many fold increase in networks and devices connected to it. It is very difficult to decrease cyber-crimes in such evolving internet unless laws in India are made strict.

Recent Attacks
"Aadhaar card bio-metrics duplicated by Axis-Bank"
The one card or the Unique Identification given to us by government has already been duplicated and misused. The government claimed it to be the safest methods for Indians to keep their bio-metrics data safe. As aadhaar uses lot of bio-metric data: from fingerprint to your retina scan to create the card and give you your aadhaar number, duplication of the card can pose a serious challenge and a threat to individuals.
All of a person's private details including our bank account and financial details, links to the other documents are saved on Aadhaar Card.
Axis Bank ltd., Suvidhaa Infoserve, E Mudhra, are leading names in the industry, these entities are guilty for Unauthorised Authentication and impersonation by using stored Aadhaar bio-metrics. They carried out transactions in the person's name by using Aadhaar card.
According to data, just one individual performed 397 bio-metric transactions between July 14, 2016 – February 19, 2017.
194 by Axis Bank
112 by E Mudhra
91 by Suvidhaa Infoserve.

"Ransom-ware Attack"
A type of malicious software designed to block access to a computer system until a sum of money is paid. The Petya/Notpetya ransom-ware is the second major global ransom-ware since WannaCry hit over 3,00,000 computers across 200 countries in May. Petya, like the recent WannaCry ransom-ware that infected over 300,000 computers worldwide, uses the Eternal Blue exploit as one of the means to propagate itself. However, experts have warned of bigger damage this time.
Pune based cyber security firm Quick Heal Technologies detected over 48,000 attempts across the country.
The WannaCry ransom-ware attack has hit about 150 countries globally, including Russia and the US. In India, five or six isolated instances have been reported in states like Gujarat, Kerala and West Bengal; though any substantial

disruption to country's IT backbone has been denied by the IT Secretary Aruna Sundararajan.
Banking Industries had to suddenly upgrade their software and settings overnight in India for safety.

What does UIDAI says?
November 11, 2016 – Unique Identification Authority of India issued some security advice through its twitter
"We urge you to be very discreet abt your aadhaar & other identity documents. Do not share the document no. Or a printed copy with anyone".
"Wherever you are submitting a copy of your aadhaar, self-attest it and state the purpose clearly to avoid misuse".
What UIDAI does not consider is that the printed or soft copy can easily be edited: may it be a picture, self-attested signature or the purpose mentioned thereupon.
Also many government and private websites forms make the aadhaar number mandatory to fill & they do not require the hard-copy say: Income Tax E-fling, PAYTM for to use its wallet service requires now individuals Aadhaar 12-digit unique identification number and since the demonetisation hit the economy businesses started accepting payments through Paytm and other e-wallets and by the current case of axis bank we are not that safe with such practices.
Even https://uidai.gov.in as on 22/07/2017 says "Do Not Share Aadhaar Number Publicly" in a big graphical text.

Current Laws for Privacy Protection and Data Security
In India
The Information Technology Act, 2000 clearly states that every business must have a privacy policy published on its website, whether or not you deal with sensitive personal data. The privacy policy needs to describe what data you collect, the purpose of the data, any third parties it might be disclosed to, and what security practices you use to protect the data. Certain sensitive data, including passwords or financial information, can't be collected or processed without the prior consent of the user.

In Argentina
Argentina's Personal Data Protection Act of 2000 applies to any individual person or legal entity within the territory of Argentina that deals with personal data. Personal data includes any kind of information that relates to individuals, except for basic information such as name, occupation, date of birth, and address.
According to Argentina's laws concerning privacy, it's only legal to handle or process personal data if the subject has given prior informed consent. Informed consent means you must tell them the purpose for gathering the data, consequences of refusing to provide the data or providing inaccurate information, and their right to access, correct, and delete the data. Also, any individual can request deletion of their data at any time.

In Australia
Australia's Privacy Principles (APP) is a collection of 13 principles guiding the handling of personal information. According to these principles, you must manage personal information in an open and transparent way, which means having a clear and up-to-date privacy policy about how you manage personal information.
Privacy policies, according to Australian law, need to detail why and how you collect personal information, the consequences for not providing personal information, how they can access and correct their own information, and how individuals can complain about a breach of the principles.
One of the roles of the Office of the Australian Information Commissioner (OAIC) is to investigate any privacy complaints about the handling of your personal information. Anyone can make a complaint to the office for free at any time, and the office will investigate as soon as possible.
In order to avoid complaints about your handling of personal information, it's important to have a clear and accurate privacy policy that includes all the requirements laid out by the APP.

In Canada
Canada's Personal Information Protection and Electronic Data Act (PIPEDA) governs how you can collect, store, and use information about users online in the course of commercial activity. According to the act, you must make information regarding your privacy policies publicly available to customers.
Your privacy policy should be easy to find and to understand, and be as specific as possible about how you collect, handle, and use information.

In Germany
The Federal Data Protection Act of 2001 states that any collection of any kind of personal data (including computer IP addresses) is prohibited unless you get the express consent of the subject. You also have to get the data directly from the subject (it's illegal to buy email lists from third parties, for example).
According to the act's Principle of Transparency section, the subject must be informed of the collection of the data and its purpose. Once the data is collected for a specific purpose, you can't use it for any other purpose without getting additional consent.
These laws apply to any collection of data on German soil, and Federal Data Protection Agency and 16 separate state data protection agencies enforce them.

In Hong Kong
Hong Kong's Personal Data Ordinance states that users must be informed of the purpose of any personal data collection, and the classes of persons the data may be transferred to (such as if you use any third-party services for processing data, like an email newsletter service).
The openness principle of the ordinance states that your personal data policies and practices must be made publicly available, including what kind of data you collect and how it's used.
If you're in violation of the Personal Data Ordinance, you could face fines up to HK$50,000 and up to 2 years in prison, and you could be sued by your users as well.

In Japan
The Personal Information Protection Act protects the rights of

individuals in regard to their personal data. The definition of personal data in the act is very broad, and even applies to information that could be found in a public directory.
The act states that you must describe as specifically as possible the purpose of the personal data you're collecting. Also, in order to share the personal data with any third party (such as an email newsletter service) you must obtain prior consent.

In Malaysia
Malaysia's Personal Data Protection Act 2010 protects any personal data collected in Malaysia from being misused. According to the act, you must obtain the consent of users before collecting their personal data or sharing it with any third parties. In order for their consent to be valid, you must give them written notice of the purpose for the data collection, their rights to request or correct their data, what class of third parties will have access to their data, and whether or not they're required to share their data and the consequences if they don't.

In Singapore
Personal data is protected under the Personal Data Protection Act. According to the act, you may only collect personal data only with the consent of the individual, and the individual must be informed of the purpose for the data collection.

In United States
In the United States, data privacy isn't as highly legislated on a federal level as most of the other countries on this list. Like with many issues, the federal government leaves a lot of the details up to each state. Laws also differ depending on the industry, which results in a confusing mess of rules and regulations for US website owners to navigate.
The FTC (Federal Trade Commission) regulates business privacy laws. They don't require privacy policies per se, but they do prohibit deceptive practices.
Some federal laws that touch on data privacy include the Health Insurance Portability and Accountability Act of 1996 (HIPAA), which deals with health-related information, and the Children's Online Privacy Protection Rule (COPPA), which applies to websites that collect data from children under the age of 13. Some states have more stringent laws than others, such as the California Online Privacy Protection Act (CalOPPA), which is the first law in the United States that specifically requires websites to post a privacy policy.
CalOPPA actually applies not just to websites based in California, but to any website that collects personal data from consumers who reside in California. With that in mind, website owners based in the United States are encouraged to err on the side of caution so they don't run into legal trouble inadvertently.
CalOPPA requires that every website that collects personal data from users post a privacy policy that includes:

- The type of personal data collected
- Any third parties you share the data with
- How users can review and change their data that you've collected
- How you'll update users of changes to your privacy policy
- Your privacy policy's effective date

If there's any chance that you'll be collecting personal data from anyone in California, it's best to comply with this law by creating an accurate privacy policy.

In United Kingdom
In the UK, the mission of the Information Commissioner's Office is to "uphold information rights in the public interest." The Data Protection Act requires fair processing of personal data, which means that you must be transparent about why you're collecting personal data and how you're going to use it. The law also states that if you use browser cookies, you need to clearly explain what they do and why you're using them, and gain the informed consent of your users.

Rejoinder to the article published in Economic Times
http://blogs.economictimes.indiatimes.com/et-commentary/let-privacy-rules-not-stifle-digitial-india-and-the-accompanying-growth-of-indias-economy/
Let privacy rules not stifle Digitial India and the accompanying growth of India's economy
July 16, 2017, 11:40 PM IST Economic Times in ET Commentary | India_|
ET By Kul dip Singh & TV Ramachandran

Begins from where it ended
"India is at the cusp of a powerful digital revolution, with rapidly growing smartphone usage and strategic government policies that promote a vibrant economy. We should recognise that it is not just our size, but also our society that has enabled us to become the world's second largest mobile market. The Internet should, therefore work for all Indians".

But at what cost?
Businesses and E Commerce have been cheating us through their privacy policies, we blindly click on I Agree, I Accept:
The OECD (Organisation of Economic Cooperation and Development) guidelines governing the protection of privacy and trans-border flows of personal data broadly describes:
The limitation principle: as to what limits the personal data should be collected.
The Purpose Specification Principle: the purposes for which personal data are collected should be specified at the time of data collection.
The Use Limitation Principle: personal data should not be disclosed, made available or otherwise used for purposes without free consent or by order of any lawful authority.
The Security Safeguard Principle: Secured form unauthorised access, destruction, use, modification or disclosure of data.
The Individual Participation Principle: individual should have the right to obtain the information about his data.
The Accountability Principle: data holder should be accountable for complying with measures of OECD Principles

Remedial Measures for India

- E-commerce and social networking sites are not held responsible because of their privacy policies which throws their responsibility to the consumers/users.
- Development of Cyber Forensics and Biometric

Techniques.
- Net Security be tightened up.
- Need for a Universal Legal Regulatory Mechanism.
- Use of Encryption Technology.
- Self-regulation by Computer and Net Users.
- E-commerce, businesses, social networking sites should be made accountable for their actions.
- Privacy rights need to be encouraged in the country. People should be made aware of their rights.
- OECD guidelines should be considered in amending the laws in India.

Privacy rights being the big issue in Whats App case: "Centre tells Supreme Court that data of the users is integral to their right to life and personal liberty".

References

1. Privacy Policy Legislation & Requirements by Country: http://privacypolicies.com/blog/privacy-law-by-country/
2. Let privacy rules not stifle Digitial India and the accompanying growth of India's economy: http://blogs.economictimes.indiatimes.com/et-commentary/let-privacy-rules-not-stifle-digitial-india-and-the-accompanying-growth-of-indias-economy/
3. Cyber Crimes Book: Orient Publishing Company.
4. Privacy Policies/ Terms and Conditions: from Instagram, Facebook, Airtel, Uber, True caller, UIDAI, Paytm applications/websites.
5. Axis Bank Case: http://timesofindia.indiatimes. com/india/probe-against-3-firms-for-illegal-use-of-aadhaar-biometrics/articleshow/57321007.cms