The Dirty Job of Data Brokerage

What is the issue?

\n\n

\n
- Multiple online profiling agencies graze on legally grey zones and collate private data without consent for commercial use.
\n
- As the problem is reaching menacing proportions, it calls for stringent regulations in the domain.
\n

\n\n

What are some of the common cases?

\n\n

\n
- Sitting in front of a computer or using a smartphone in the comfort of our homes, we might think that the world doesn't know what you are up to.
\n
- But every click online creates an indelible data trail that is being capitalised by data hawks who've set up the infrastructure to monetise on them.
\n
- This intrusive trend can significantly compromise ones health status, schedules, food and sleep habits, educational profile etc...
\n
- Broadly there are two modules that are used for data mining from unsuspecting users, who happen to part with their data.
\n
- **Cloud Breach -** Information shared through e-mail is thought to be inherently secretive and that only the intended receivers get access to it.
\n
- But information gets regularly breached and shocking cases of "add targeting" based on the content of personal e-mails have also come up.
\n
- Notably, one of the contenders claimed that he disclosed his planned tour only to a firend over mail, which has his browser being flooded with related ads.
\n

- Hence, even harmless data about your itineraries, your financial statements etc, that is stored in your personal email cloud might not be all that secure.
\n
- **Data Brokering -** Applicaitons that compare and contrast various services presently aplenty online, most of which don't have a clear data protection law.
\n
- These applications demand some basic contact information as a pre-requisite for accessing their services, which most users willing part with.
\n
- In many cases contact information is then outrightly sold by the promoters of the applications to marketers of the products you've been looking for.
\n
- Notably, sometimes even direct marketing calls are made if phone number had been inadvertently provided.
\n

\n\n

How does the data-brokerage landscape look worldwide?

\n\n

\n
- Nearly 10 million open datasets are published by government agencies and non-governmental organisations (NGOs), annually.
\n
- While there are data sets that actually are aggregated with the concent of the user, the landscape is dominated by unauthorised accumulators.
\n
- Data brokers are companies that sell personal information of individuals online and there are an estimated 5,000 data brokers worldwide.
\n
- Incidentally, no data-brokering firms claims them to be one and rather they use fancy names for their services like - "customer engagement, data research, information services or marketing automation".
\n
- But their work is the same - collecting data about individuals from many sources without consent from those who are profiled.
\n
- Crime investigators and data brokers actually perform a similar task – while the former profiles criminals to nab them, the latter works to target the public with suitable ads.
\n

\n\n

What are the challenges in the field?

\n\n

\n
- **Data Theft -** Fraudulent websites that resemble the real ones are often set up where the unsuspecting online visitor will generously offer his or her details.
\n
- But crack down on clones of even hugely popular online games like Temple Run and sites such as Flipkart, WhatsApp, Facebook has been lukewarm.
\n
- Data is also easily scraped from websites with poor security policies by hackers or even out-rightly sold by the promoters without consent.
\n
- Sometimes unsuspecting users don’t realise the implications of giving out their data on unsecure platforms and liberally share personal information.
\n
- **Legal Gaps -** Data brokering as such is not illegal but it does fall in a grey zone as the legal recourse in this regard is vaguely articulated at present.
\n

\n\n

\n
- Currently, provisions of the Information Technology Amended Act, 2008 (ITAA) is what governs the data framework in India.
\n
- While a stand alone “Personal Data Protection Bill” is under consideration to strengthen regulations, it may still take some time to come into force.
\n
- EU and Japan have laws that mandated consent of a data subjects in case of transmitting data to a third party or diverting it for unstated purposes.
\n
- There are also provisions that establish significant liabilities on data controllers, and individuals are entitled to compensations in case of a breach.
\n

\n\n

What is the way ahead?

\n\n

\n
- Considering the potential implications of this new phenomenon – the policy makers and all other stakeholders need to be invested in finding a solution.
\n

- Organisations too need to look at the ethical considerations in collecting, storing and sharing data in a way that does not compromise individual privacy.
  \n
- At an individual level, being more alert while leaving a digital footprint will go a long way in protecting one’s privacy and individual interests.
  \n
- Using ad blockers, disabling third-party apps, auditing social media accounts and not sharing personal details at random online and offline sites are key.
  \n
- It is also very important to educate and raise awareness in this domain among the younger generation.
  \n

\n\n

\n\n

Source: Business Line

\n\n

\n