The right to privacy
- A feminist perspective

Anita Gurumurthy
IT for Change

1. Privacy and the platform publics of the twenty first century
2. Carving out a right to privacy in the new public sphere
3. Techno-policy considerations in interpreting the right to privacy

1. Privacy and the platform publics of the twenty first century

The public-private distinction in the evolution of the doctrine of privacy

A division between the public sphere of political affairs (termed the polis) and the personal sphere of human life including family life (termed oikos).

- Aristotle, Ancient Greek Philosopher

Castle Doctrine: “For a man's house is his castle, et domus sua cuique est tutissimum refugium [and each man's home is his safest refuge].”

- Sir Edward Coke, The Institutes of the Laws of England, 1628

The public-private distinction in the evolution of the doctrine of privacy

Zone of Liberty from the State: “The only part of the conduct of any one, for which he is amenable to society, is that which concerns others. In the part which merely concerns himself, his independence is, of right, absolute. Over himself, over his own body and mind, the individual is sovereign.”

- J.S. Mill, On Liberty (1859)

Right to be left alone/ inviolate personhood: “The principle which protects personal writings and all other personal productions, not against theft and physical appropriation, but against publication in any form, is in reality not the principle of private property, but that of an inviolate personality.”

- Warren and Brandeis, “The Right to Privacy”, Harvard Law Review (1890)

How Privacy is Negotiated

In the public sphere

- Shared ideas about privacy in a society allows freedom of conscience and diversity in thought. These public values guarantee democratic participation, including freedoms of speech and association, and checks on government power - Priscilla Regan, Legislating Privacy (1995)
- Guaranteed through the constitution and statutory rights including, against self-incrimination, as personality rights (right of publicity, copyright & other IP), in fiduciary contexts (doctor-patient, financial advisor)
- A market in which these boundaries between public & private are managed

Data is the new four letter word-
We are because we are tracked!

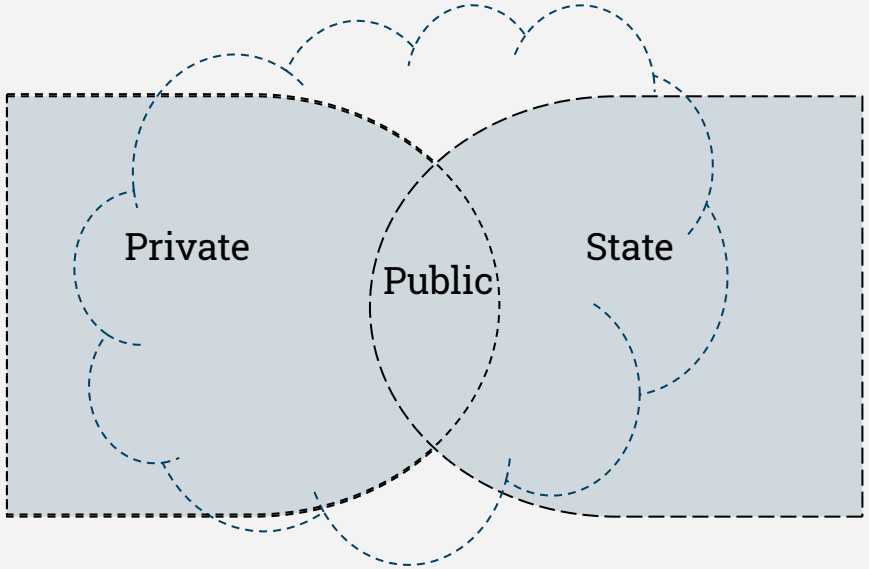
The 21st Century has seen an explosive growth in the volume, velocity and variety of data production… We are seeing the datafication of all bodies

“Information and data flow are “increasingly central to social and economic ordering”. Individuals are identified with reference to tax records, voting eligibility, and government-provided entitlements.” - Puttaswamy v U.o.I (Aug 2017)

The all-pervasive data regime is transforming every social institution and activity

In a neo-liberal society, the previously immaterial labour of digital users – is converted into behavioural data sets, expropriated by private profit.

Platformised-Public



Digital Technology has led to the birth of a new space for social exchange: a quasi-public sphere

The State of the New Quasi-Publics

Anonymity

Virality

Fragmentation

-Frank Pasquale

Manipulation of voters through algorithmic profiling

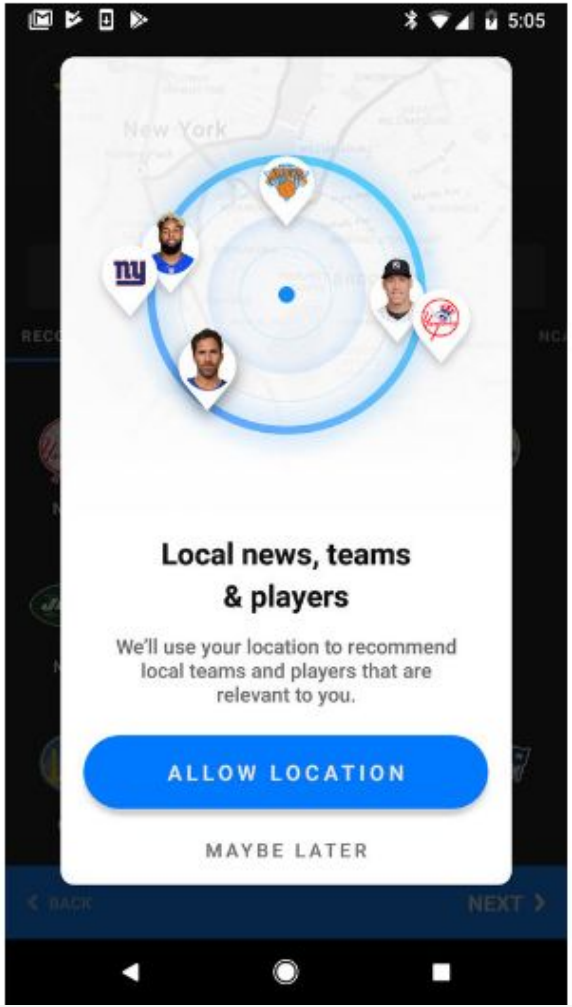
Online virality as the metric of success regardless of quality or truth

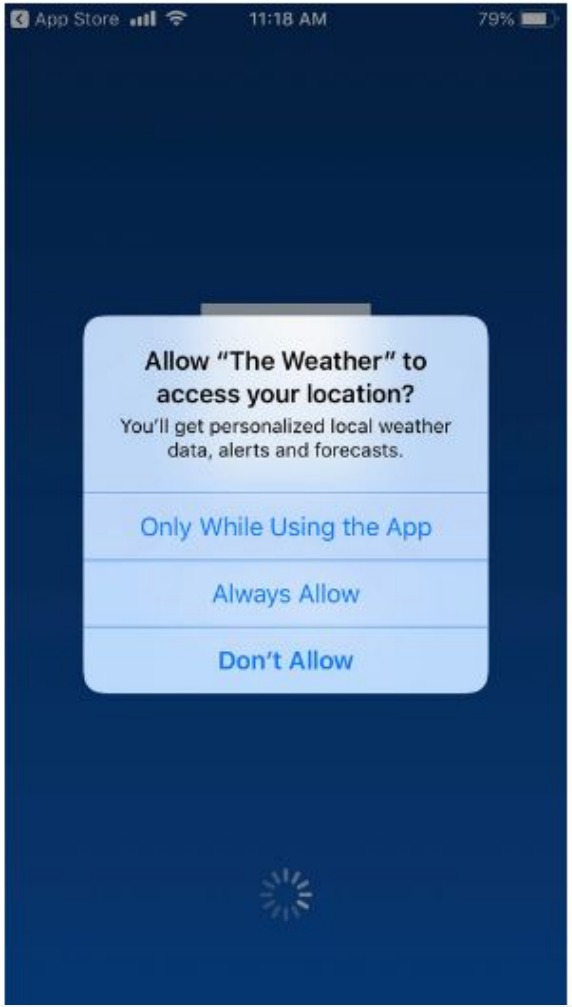
Elevating profit considerations over democratising functions of public discourse

The market for trading in any(every)one's privacy

- Many of our most important sites of commerce are markets for information
- 'Dark ads' and sophisticated personalisation algorithms enable constant experimentation on unwitting human research subjects, so A/B testing (particularly when used to measure divergent responses among thousands of users) can reveal exactly what manipulation works best. Without conscientious and professional curation of such algorithmic orderings of information, the public sphere's automation is susceptible to distortion by the most well-resourced entities.

- Frank Pasquale





Most People Don't know What's Going On

The market for trading in any(every)one's privacy

- Privileging market interest - "blanket and frictionless **consent"**
- Increasing resolution of privacy contestations through **contract** law - say for eg. Terms of Reference in FB or Apple device
- The role of PDP is about putting down the minimum threshold above which an individual consumer can sign away her privacy.
- Informational, decisional, physical autonomy

Porous private-public

Platform terms of use/ community standards - arbitrary/ad hoc governance -

- Facebook - Cambridge Analytica
- Zoom - E2EE sought to be restricted to paid users

State overreach owing to absence of law -

- Mass surveillance not seen as an unconditional privacy violation (Big Brother Watch v. Secretary of State (ECHR 2018))

2. Carving out a right to privacy for a new public sphere

Findings from IT for Change' study - Righting Gender Wrongs

Finding 1.

Cyberspace is home to pervasive sexism - one-third of survey respondents have faced harassment, abuse or unwanted behaviour online and two-fifth are aware of other women in their circles who have had similar experiences

90%

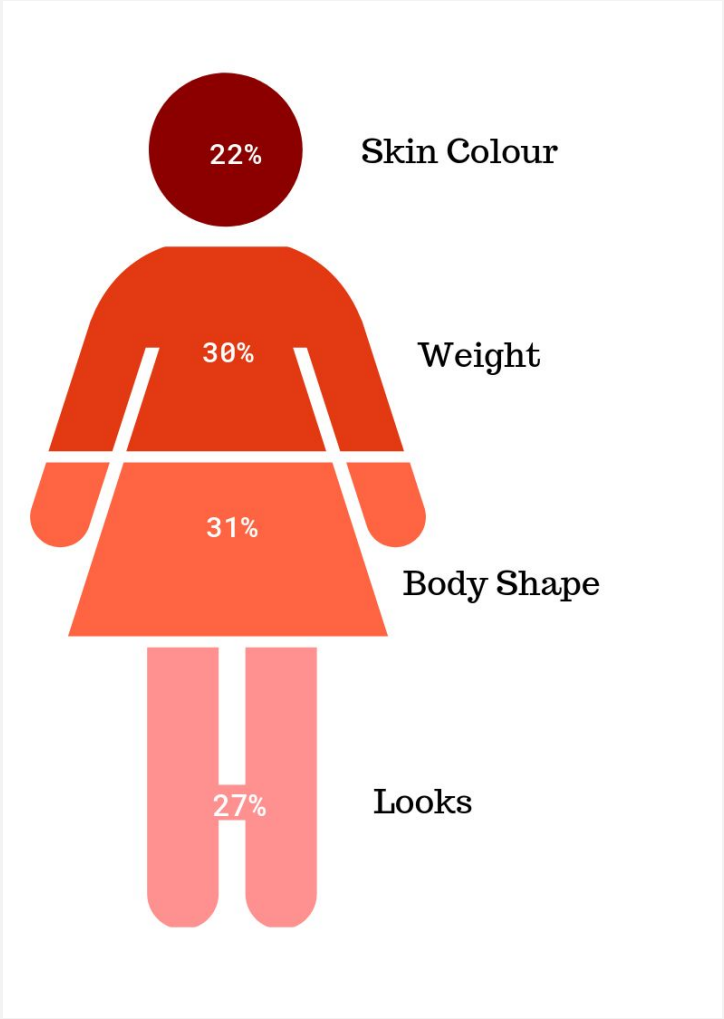
of survey respondents who faced harassment, faced it on multiple occasions.

Findings from ITfC study

Finding 2.

Over three-fourth of respondents have faced gendertrolling -

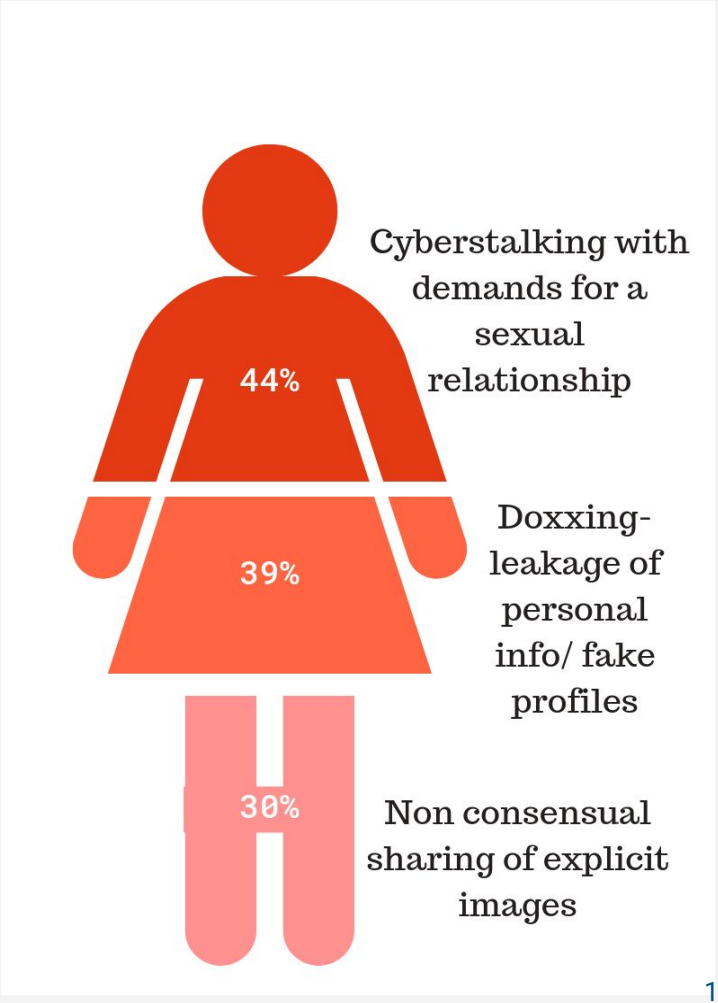
Women from marginal social locations face particularly heinous forms of gendertrolling that denigrate their social identity. Misogynistic vitriol faced by dalit women is also casteist.



Findings from ITfC Study

Finding 3.

Over 80% have faced online sexual harassment of some form. Cyberstalking, doxxing and cyberflashing are distressingly common



"I took the ‘Cinderella’ approach. My Facebook account was safer than the Swiss Bank! There are no men on it, except a cousin, and a boring friend of my father’s.

…When I started responding to people’s comments, I would comment, and then deactivate because I was scared of what the response would be. I was scared to put up a profile picture. I added one only after becoming a researcher.”

“My boyfriend saw a pic of mine sitting with my thigh upon the other thigh. He told me I should not pose for pics like that. Put both feet on the floor.”

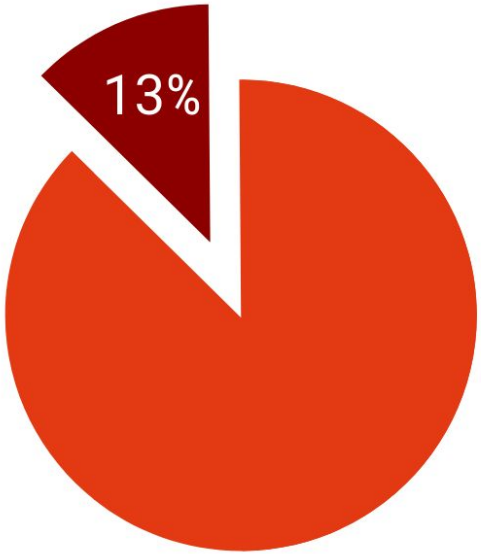
“But girls also should keep their accounts private and within their friends’ circle. They should be more careful. If they are concerned, why aren’t they more careful? There are a lot of ways to do this now. You can share things with only a group of friends. But girls want likes and fame. That may be a problem.”

“Girls should dress properly when they post music videos on TikTok. If they don’t, they should not complain about any misogynist counter-video posted to tease them.”

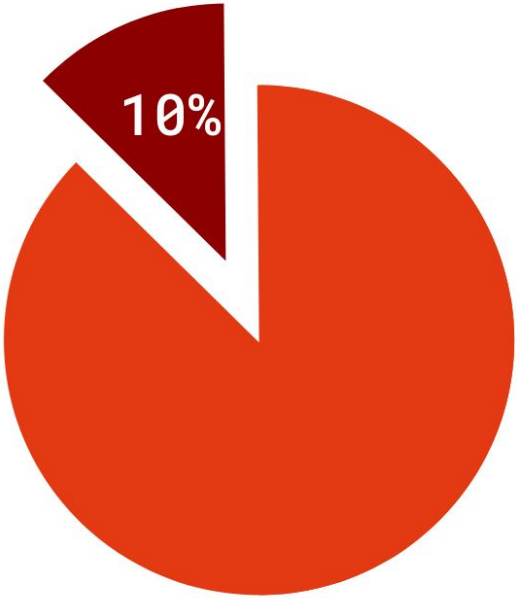
Quitting the web is not an option.
The space of individuation is too precious and so young women must manage their voice and visibility responsibly.

22

Very few women victims approached college authorities



Despite facing cyberviolence, very few women approached the police



Privacy in the new public sphere

Autonomy: Informational, decisional, bodily, associational, communicative, intellectual, behavioural, spatial autonomies in online spaces.

Dignity: The need for an account of **harms** that take place in the intimate-private / private-corporate spaces of the online publics.

Equality: The need for reckoning with the context in which privacy is at risk.

“The challenge in this area is to enable the state to take the violation of the dignity of women in the domestic sphere seriously while at the same time protecting the privacy entitlements of women grounded in the identity of gender and liberty.”

Justice K.S. Puttaswamy v Union of India (24 Aug, 2017)

So, privacy is not only about freedom from surveillance (state and market)

But also tied to dignity in the intimate spaces of the online public sphere

How the market and its AI tools fail women

Revenge Porn of non-consensual circulation of intimate images (NCII) - In many jurisdictions, copyright issues are taken up by platforms with more seriousness than other issues

FB claims that the cultural variations in what is an “intimate image” makes it hard for them to train their AI

Limits of AI tools

Facebook AI filter unable to flag advocacy of violence against women.

This is especially compounded in vernacular languages spoken and written in India

Privacy & Dignity in the IT Act and IPC

Cyberstalking - 354A IPC (stalking), or 67 (obscenity) IT Act

Trolling - 509 IPC (outrage of modesty)

Doxxing - the law does not capture this.

66E - covers ‘bodily privacy’, but defined only to mean images of a private part of a woman

67 and 67 A - anti-obscenity - focuses on “whoever publishes”- also, no conception of multi-layered consent separately for capture, sharing, dissemination in every instance

Content Takedown & Responsibilizing Intermediaries under the IT Act, 2000

Section 79 - due diligence of intermediaries under Intermediary Guidelines, 2011

Section 66A - ambiguity around “grossly offensive”

Effect of *Shreya Singhal* on Sections 79 and 66A

- 79 - obligation of removal only upon court order
- 66A - struck down as vague & arbitrary

Notice & Takedown regime does not account for Non-Consensual Circulation of Intimate Images (NCII), gender based hate speech

Indecent Representation of Women Act amended 2018- now has a digital component

Privacy in the new public sphere

From a feminist standpoint where “personal is political”, privacy considerations in a democracy must pass the test from two ends.

Individuals must be seen as having legitimate interests in personal as well as political forms of freedom and equality.

AND SO, the right to privacy must imply both a common minimum standard of informational, decisional and physical privacy (a room of one's own) vital for a flourishing public-political life as well as a duty for publicity commensurate with social power (given that individuals cannot have much the same needs for privacy)

https://www.genderit.org/articles/data-new-four-letter-word-feminism

Privacy & Dignity infringements are not mere contractual infirmities

FTC decision on "revenge" pornography website, MyEx.com (Emp Media Inc.) - is copyright enough?

The website allowed individuals to submit intimate photos of the victims, including personal information such as name, address, phone number and social media accounts. If a victim wanted their photos and information removed from the website, the defendants reportedly charged fees of $499 to $2,800 to do so.

FTC ordered shutdown of the website and permanently prohibited the defendants from posting intimate photos and personal information of other individuals without their consent. The defendants were also ordered to pay more than $2 million.

3. Techno-policy considerations in interpreting the right to privacy

Interpreting the Right to Privacy

The 34th Session of the **UN Human Rights Council** (Mar 2017) adopted the resolution on “**right to privacy in the digital age**” (A/HRC/34/L.7/Rev.1), which has crucially insisted on States ensuring “that any interference with the right to privacy is consistent with the principles of **legality, necessity and proportionality”.**

Interpreting the Right to Privacy

Necessity, Proportionality, Legitimacy

Vinit Kumar versus Central Bureau of Investigations and Ors (Bom HC, 2019), Bombay High Court outlined the scope of the state's power of surveillance - An order of communication interception under section 5(2) of the Indian Telegraph Act can only be given in situations of 'public emergency' or 'public safety'.

Indian Hotel and Restaurant Association (AHAR) and Ors. vs. The State of Maharashtra and Ors., 2019 (Supreme Court) - Maharashtra Act on Dance Bars - Several of the conditions under the Act were challenged, including one that required the installation of CCTV cameras in the rooms where dances were to be performed. Here, the Court relied on Puttaswamy (and the discussion on unpopular privacy laws) to set aside the condition requiring such installation of CCTV cameras.

“Courts, in order to decide a case, must carry out a balancing operation, weighing the public interest in maintaining confidence against a countervailing public interest favouring disclosure.”

Justice K.S. Puttaswamy v Union of India (24 Aug, 2017)

Bulk Interception in times of Panspectronic State

Big Brother Watch v. Secretary of State [2018] ECHR 722 (ECHR)

Secret surveillance regimes including the bulk interception of external communications violated Articles 8 (exhaustion of domestic remedies) and 10 of the Convention for the Protection of Human Rights and Fundamental Freedoms.

“in view of the potential **chilling effect** that any perceived interference with the confidentiality of their communications and, in particular, their sources might have on the freedom of the press and, in the absence of any "**above the waterline**" arrangements **limiting** the intelligence services' ability to search and examine such material other than where "it is **justified** by an overriding requirement in the public interest", the Court finds that there has also been a violation of Article 10 of the Convention.”

Data & the Role of Platforms

- Targeted Advertising
- Mass Surveillance
- Encryption
- Hate Speech
- Fake News

Tech Design

The Irish DPC issued new guidelines at the end of 2019 - increasing focus on the requirements of privacy by design and default.

In 2018, FTC enforcement actions led to large settlements with technology manufacturers Lenovo and Vizio.

- Lenovo ordered to obtain affirmative consent from consumers before running the software on their computers and implement a software security program on preloaded software for the next 20 years.

- Vizio agreed to pay $2.2 million, delete the collected data, disclose all data collection and sharing practices, obtain express consent from consumers to collect or share their data, and implement a data security program.

Privacy Enhancing Technologies

The ability to lock your profile is a feature of FB designed for people in India, especially women. Stalkers will not be able to zoom into photos or save them. They will also not be able to see photos and posts on the timeline (both historic and new) either. But one can't post to the "public" when one's profile is locked. (May 21, 2020)

Instagram rolled out new mode called "Restrict" that lets account owners effectively shadow ban a user who comments on photos with offensive or abusive language (July, 2019)

The Debate on Encryption- Right to Privacy versus Right to Securely Govern the State

End-to-End Encryption on WhatsApp

Madras HC Whatsapp Traceability Case (2019) - now in SC

Tamil Nadu Advocate General: “We were asked to submit the problems we are facing in criminal investigations, and we have done that. The social media companies don’t give us the relevant information. There are too many delays.” “We need their cooperation to find perpetrators.” “We want the social media companies to decrypt and give us the information.”

IT for Change Study (2018)

It takes a long time; police request for evidence, Facebook takes 20 days, then FB asks for more information, police responds and again, FB takes 20 days to respond. This negatively impacts the investigation process.

GDPR and the PDP Bill

Personal Data Protection Bill, 2019 provides

Expansion of the definition of personal data to include inferred data (Section 3(28)) - missing in the text of the GDPR

The introduction of a right to erasure (Section 18) - which is combined with a right to be forgotten in the GDPR

Notifying the class of ‘significant data fiduciaries’ for data protection impact assessment (Section 27) - not in the GDPR

A ‘privacy by design’ policy (Section 22) - wider than in the GDPR

GDPR and the PDP Bill

Gaps

PDP Bill 2019 does not recognize the power asymmetry between the employer and the employee.

PDP Bill makes it possible to completely exempt state agencies from the effects of the PDP law, making it ineffectual against the state

Once a fundamental right to privacy has been guaranteed, the right to privacy is to evolve on a case to case basis, and as a fundamental human right, "should only yield to State action, if such State action is compelling, necessary and in public interest".

Justice K.S. Puttaswamy v Union of India (24 Aug, 2017)

Surveillance beyond Personal Data Protection

Privacy and data protection laws are not an effective fix to the surveillance tendencies of modern states and the market.

- Facial Recognition Technologies - e.g AFRS
- DNA Profiling
- Bio resources

Not enough to just guarantee protection of personal data

Alternative ideas of data governance that address the datafication of society, economy and polity must be introduced into the law - Content Moderation, Algorithmic Governance, Non Personal Data, Antitrust