Privacy and ethics

Altman et al., in the paper "*Practical approaches to big data privacy over time*" broadly talk about privacy controls in a research context vs those in government/commercial settings. The paper correctly states that the stringent legal and regulatory frameworks for research involving human subjects leads to systematic handling of the data. Consider for example, clinical trials. Clinical Data Management, in compliance with regulatory standards such as HIPAA, is not only a major step in the process, it is of utmost importance to maintain an audit trail of the data management activities for better traceability and transparency.

However, such stringent mandates do not exist in the business or government context. To give an example, you would be surprised to know that a few months back, India withdrew its Data Protection Bill, which was introduced as late as 2019 in the first place. As a result, the world's largest democracy is back to square one with no protection from organizations storing and using personal information. It is also because of this absence of a data protection law that WhatsApp's updated privacy policy which allowed for user data from chats with business accounts to be shared with third-party apps including Facebook has been put on hold in India.

It is true that businesses "in most cases they do not engage in systematic and continual review with long-term risks in mind." As a result, they end up storing PII for longer periods of time, thus leading to increased risks of cyber-crimes. An Indian ed-tech startup, Byju's, ended up being the victim of two such cyber-crimes in period of six months. This company stored personal information including, but not limited to, name, email, age, phone number, chats, video and audio recordings between students/parents and tutors. All of this information was leaked from their servers in a data breach.

The authors correctly point out that "Consumers often do not read or understand privacy policies, and the terms of such policies are often written so broadly or vaguely as to not fully inform those who do read them." For the purpose of this response, I read the privacy laws of WhatsApp and I have to admit that I not only thought that they are written in a vague manner but also found them ambiguous to interpret. Moreover, a 2019 Pew survey[1] found that only 9% of Americans always read privacy policies. It makes sense given the fact that one who wishes to use the app/service does not really have an option but to agree to the policy.

Nissenbaum, in the article "*A Contextual Approach to Privacy*", brings out an interesting point of laws being applicable to offline vs online channels. A law which protects someone from stalking may not be sufficient to protect someone from cyber-stalking. Given the number of social media channels today, there can be numerous activities which constitute cyber-stalking. It goes back to the Moor's article[2] from first week which talks about "policy vacuums". In such situations which have presence in both online and offline world, it is thus important to make sure that the laws are extended to cater to all cases. Nissenbaum rightly suggests that it is are more challenging to create explicit laws and policies for contexts which are specific to the Net, such as Metaverse, cryptocurrency, NFT etc.

Researchers, organizations, and governments should follow suit from GDPR, which sets a high standard for consent, privacy, and protection of consumers' data.

[1] 2019 Pew Research, https://www.pewresearch.org/internet/2019/11/15/americans-attitudes-and-experiences-with-privacy-policies-and-laws/
[2] James H. Moor, *"Why we need better ethics for emerging technologies"*