Data Ethics Professional webinar #8: personal data security and dark pattern with Ramon Abraham Sarmiento

Wednesday 17 September 2025, 9:30 am BST

Today's Speakers

Ramon Abraham Aquino Sarmiento

Ramon "Mon" Abraham Aquino Sarmiento, is a government lawyer with over 15 years of experience in data governance, data privacy, ethics, and policy development.

He currently serves as Deputy Director at the Bangko Sentral ng Pilipinas, where he also acts as the Data Protection Officer and Big Data Steward for the Monetary and Economics Sector.

Chair

Dr Kay Achenbach, Senior Learning Specialist and Head of Data Ethics, The ODI

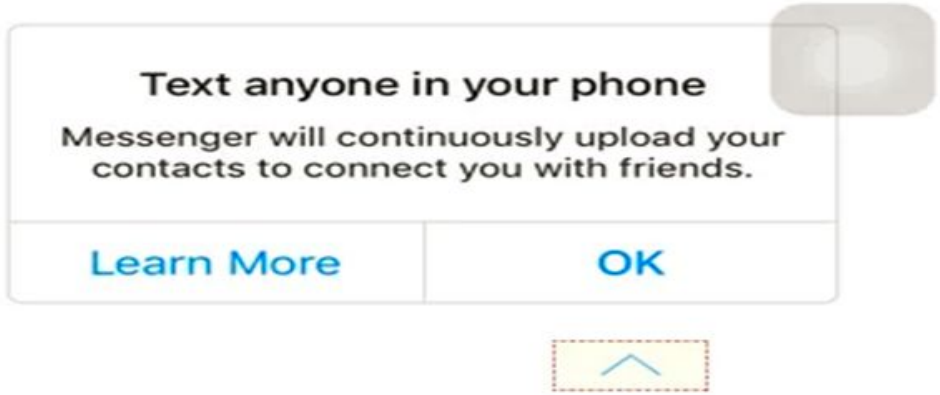
Outline

1. Literature Review
2. The Ethical and Legal Frameworks
3. Regulatory Gaps and Possible Solutions

Literature Review – Dark Pattern

"A Dark Pattern is a manipulative or deceptive trick in software that gets users to complete an action that they would not otherwise have done, if they had understood it or had a choice at the time. For example if you have a button that functions as a "Yes" when clicked, but through the use of placement, colour and trick wording, it appears to say "No", then many users are going to be caught out." – Harry Brignull

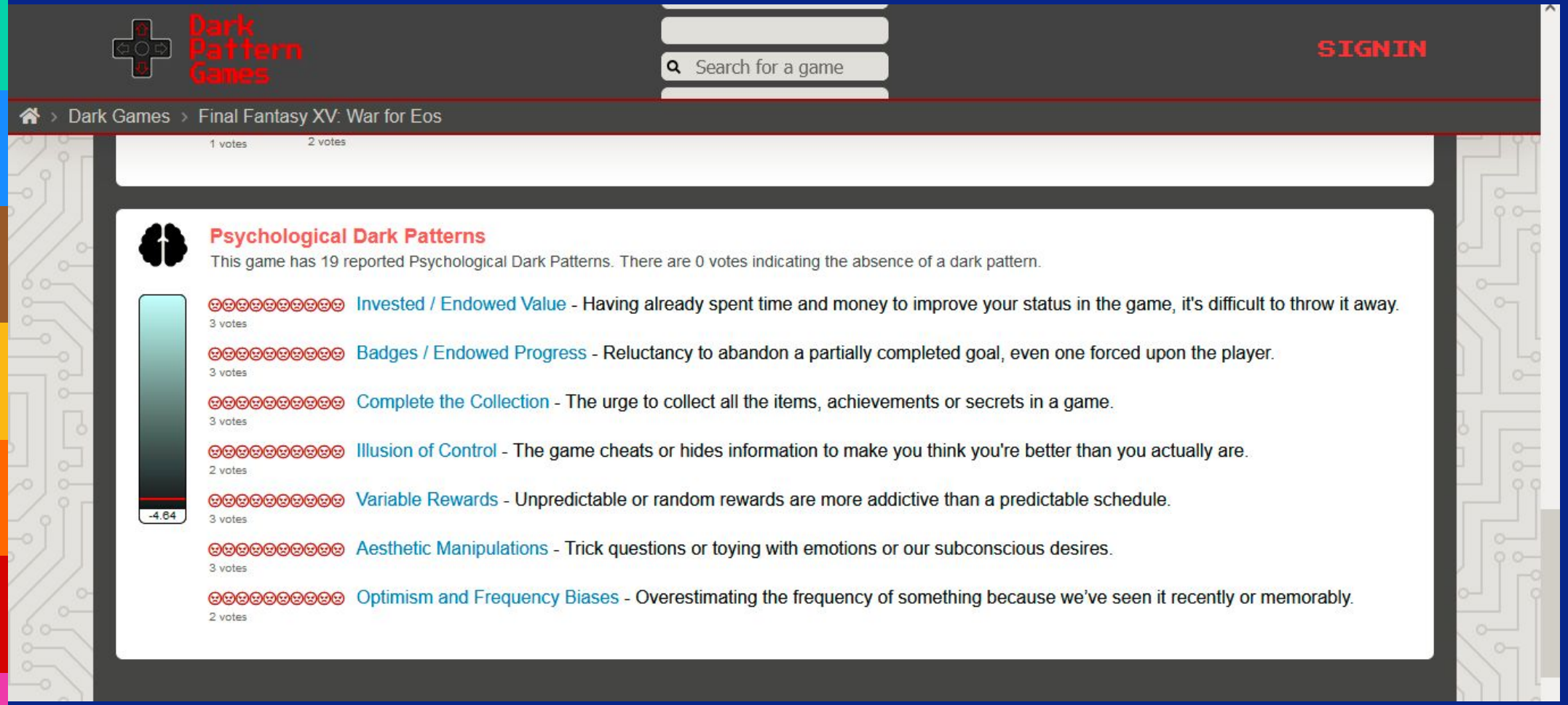
Literature Review – Dark Pattern



Syncing your contacts helps friends connect on Facebook, too. Manage contacts.

Fig 1 →Screenshot of Facebook-messenger application on iOS (while installing messenger on iPhone). Focus on the additional blue arrow (highlighted) and missing cancel option

Literature Review – Dark Pattern



Literature Review – Dark Pattern

- At least 19 different definitions of dark patterns;
- Shares similarities and often intersects with the studies on online manipulation, malicious interfaces, nudges, surveillance capitalism and UX design; &
- Prevents users from making conscious, informed decisions about the management of their personal data which in turn exposes them to a number of risks and harms, including cyberstalking, identity theft and reputational damage.

Literature Review – Dark Pattern

A large-scale experiment conducted by on census-weighted samples of American adults showed that mild dark patterns more than doubled the percentage of consumers who signed up for a dubious identity theft protection service, and aggressive dark patterns nearly quadrupled the percentage of consumers signing up (Luguri & Strahilevitz 2021).

Literature Review – Dark Pattern

- Privacy Zuckering,
- Bad Defaults,
- Forced Registration,
- Hidden Legalese Stipulations,
- Immortal Accounts,
- Address Book Leeching. and
- Shadow User Profiles.

Literature Review – Dark Pattern

Dark patterns and privacy intrusive defaults, would nudge users of Facebook and Google, and to a lesser degree Windows 10, toward the least privacy friendly options to an unethical degree (Forbrukerrådet, 2018).

Literature Review – Dark Pattern

Di Geronimo et. al. (2020) found that 95% of 240 popular mobile applications contained one or more dark patterns, and on average 7.4 dark patterns.

For the Japanese app context, Hidaka et. al. (2023) found that 93% of 200 popular Japanese mobile applications contained one or more dark patterns, and on average they contained 3.9 dark patterns.

Literature Review – Dark Pattern

Kowalczyk et. al. (2023) found at least 3 unique dark patterns in all 57 Internet-of-Things (IoT) devices studied and on each IOT devices contained an average of over 25 dark patterns

Literature Review – Dark Pattern

Marti et. al. (2024), found 186,892 companies sent data about 709 volunteers to Facebook. Each volunteer had an average of 2,230 companies sharing their data with Facebook and some volunteers had over 7,000 companies providing their data.

Literature Review – Dark Pattern

Rubenstein (2013) argued that the advancing wave of big data will overwhelm the informed choice model.

Literature Review – Disclosure Risks

Although disclosure may seem difficult for an isolated dataset with supposedly "anonymized" data, re-identification can be performed by linking public records such as voter registration records, with de-identified data (Dwork et. al. 2017).

Literature Review – Disclosure Risks

- AOL users,
- Netflix Users,
- Harvard Class of 2009,
- Australian de-identified open health dataset,
- Victorian Government transport dataset, &
- Washington State, Vermont and Maine patient-level health datasets.

Literature Review – Disclosure Risks

Census Bureau in preparation to the 2020 Census showed 53% of respondent were concerned about the confidentiality of their census responses. Of these concerned respondents, 28% were "extremely concerned" or "very concerned" and a further 25% were "somewhat concerned" about the confidentiality of their census responses (McGeeney et. al. 2019).

Literature Review – Disclosure Risks

A 2023 survey by Pew Research showed 84% were very worried or somewhat worried that companies selling your information to others without you knowing.

Literature Review – Disclosure Risks

Sherman et. al. (2021) found that U.S. data brokerage industry gathers data on virtually every American, by scraping public records, embedding code into mobile apps, and purchasing customers data from various companies.

Literature Review – Disclosure Risks

Athey et. al. (2018) research indicates that even small monetary incentives this leads individuals to surrendering their personal information and drives platforms to gather increased information. They further posit that this may undermine the efficacy of regulation.

Literature Review – Disclosure Risks

Individuals are unable to accurately price their personal information in relation to the cost of surrendering it despite the prevalent negative attitudes towards this surrender of personal information. Spiekermann et. al. (2015) even speculated that knowledge of the volume and business done with their data among third parties, may lead individuals to be surprised and feel betrayed.

Estimating Reidentification Risks of Dark Patterns in Philippine Survey Data

- DB to Data offers Philippine call lists with prices ranging from USD 150.00 for a list of 10,000.00 to USD 4,000.00 for a list of 3,000,000.00.
- Email lists of 10,000,000 Filipinos for USD 400.00

Estimating Reidentification Risks of Dark Patterns in Philippine Survey Data

- DB to Data offers Philippine call lists with prices ranging from USD 150.00 for a list of 10,000.00 to USD 4,000.00 for a list of 3,000,000.00.
- Email lists of 10,000,000 Filipinos for USD 400.00

Estimating Reidentification Risks of Dark Patterns in Philippine Survey Data

These are just the small-fry, in 2020, Axciom, one of the biggest data brokers, declared that is has "*the largest depth and breadth of demographic segmentation and predictive data, identifying over 260 million US consumer portraits.*"

The Ethical and Legal Frameworks

In addition to any legal obligations to do so, many researcher routinely promise anonymity to subjects who participate in studies or surveys (Heffetz & Ligett).

The Ethical and Legal Frameworks

These promise of anonymity hold immense value to respondents, as a survey by Hotz and Slanchev (2017) showed that 79.5% of respondents cited confidence in researchers to keep responses and information private" as the most important determinant for their participation in a hypothetical study.

Minimization of Disclosure Risks

The United Nations General Assembly adopted the Fundamental Principles of Official Statistics in January 2014. Principle 6 of which states: *"Individual data collected by statistical agencies for statistical compilation, whether they refer to natural or legal persons, are to be strictly confidential and used exclusively for statistical purposes."* The adoption and implementation of these principles is in various national laws, overviews of which can found on the United Nations Statistical Division website.

Minimization of Disclosure Risks

- The Privacy Act of 1974;
- The HIPAA;
- Title 13 of the U.S. Code;
- CIPSEA
- Chapter V of Commission Regulation (EC) No 223/2009
- EU Regulation No 557/2013
- European Data Governance Act

Minimization of Disclosure Risks

Criminal penalties for unauthorized re-identification of anonymized information.

- Section 48F of the Singapore's Personal Data Protection Act 2012; &
- Section 171 of the United Kingdom's Data Protection Act 2018

Regulation of Dark Patterns

- The California Consumer Privacy Act (CCPA);
- The Connecticut Data Privacy Act;
- The Colorado Privacy Act;
- The Vermont Data Privacy Act;
- The California Age-Appropriate Design Code Act (CAADCA);
- The Federal Trade Commission Act, 15 U.S.C. § 57a(a)(1)(b)
- EU GDPR
- EU Guidelines 03/2022 on Deceptive Design Patterns in Social Media Platform Interfaces
- EU Digital Services Act

Regulation of Dark Patterns

Section 1798.140.l of California Consumer Privacy Act (CCPA) defines dark patterns as a "user interface designed or manipulated with the substantial effect of subverting or impairing user autonomy, decision making, or choice, as further defined by regulation."

Sale of Personal Data and Data Brokers

- Lightly regulated if at all.
- GDPR.
- California Privacy Rights Act (CPRA).
- California Delete Act.
- Bureau of Consumer Financial Protection.

Regulatory Gaps

Oberski & Kreuter (2020) have proposed that de-identification policy should be like cybersecurity policy, since perfect, impregnable security is impossible, it follows that de-identification and data security policy should minimize the risk of breaches and other failures down to acceptably low levels. The regulatory goal should be ensuring the widest number of data custodians reduce such risks to the lowest possible degree, while still retaining the utility of sharing data. Closing the regulatory gaps regarding dark patterns would contribute to this regulatory goal.

Regulatory Gaps

Research conducted by Di Geronimo et. al. (2020) shows that 55% of users did not spot malicious designs in applications containing dark patterns, 20% were unsure, and the remaining 25% found a malicious design.

Regulatory Gaps

The OECD (2022) finds that there could be gaps in the law, in available evidence, or in enforcement capacity since enforcement cases predominantly relate to a few dark patterns commonly recognized by regulators.

Regulatory Gaps

Many surveys show people have a strong distaste for the sale of their data and given the openness of the sale of these data sets, it would be fair to conclude that a sizable portion was sourced using dark patterns. Absent more detailed studies on the prevalence of data sets assembled by privacy-infringing dark patterns, commercial data sets that can be purchased with little or no limitations, are a reasonable proxy for illustrating disclosure risks in relation to the prevalence of dark patterns

Regulatory Gaps

- Light enforcement of the Do Not Sell provisions of the CCPA by registered data brokers in California.
- Some brokers seemingly resorted to dark patterns to get consumers not to exercise their right not to have their data sold.
- The dark pattern sourced data in these datasets were allowed to build up over years with scant regulation.

Regulatory Gaps

Knowing how much dark pattern-sourced data is out there is especially important for research where current protection methods such as differential privacy are not appropriate such as demographers, redistricting analysts, or immigration

Regulatory Gaps

Knowing how much dark pattern-sourced data is out there is especially important for research where current protection methods such as differential privacy are not appropriate such as demographers, redistricting analysts, or immigration

Conclusion

Dark patterns are by no means the only factor in the ongoing debate between protecting privacy and utilizing datasets in the age of big data, but they should still be considered in view of their prevalence and scant regulation. Understanding the gaps in the regulations of these dark patterns should be a key subject for researchers and policy makers as such knowledge will enable society at large better utilize the enormous and varied data sets that fuel big data.