Consent as an Instrument to Protect User Privacy

Rishab Bailey
National Institute of Public Finance and Policy

July 2019

Outline

- Exercise
- Introduction to the concept of "consent"
- Criticisms of the 'notice-consent' framework in the privacy context
- Paper: *Disclosures in privacy policies: Does notice and consent work?*
  - Analysis of policies
  - Survey
- Consent related provisions in the draft Personal Data Protection Bill, 2018
- How to improve notice and consent mechanisms
- Conclusions

Exercise - Replicating our Survey

Exercise

- Please read the privacy policy you have been provided
- Please answer all ten questions in the survey
- Appropriate answers: Yes / No / Not specified / Can't say

The Correct Answers

1. –> Not specified – NA – 25 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent
5. –> Yes – lines 113-122 - 75 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent
5. –> Yes – lines 113-122 - 75 percent
6. –> Not specified – (lines 159-156) – 46 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent
5. –> Yes – lines 113-122 - 75 percent
6. –> Not specified – (lines 159-156) – 46 percent
7. –> Not specified – (lines 143-144) – 41 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent
5. –> Yes – lines 113-122 - 75 percent
6. –> Not specified – (lines 159-156) – 46 percent
7. –> Not specified – (lines 143-144) – 41 percent
8. –> Not specified – NA – 37 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent
5. –> Yes – lines 113-122 - 75 percent
6. –> Not specified – (lines 159-156) – 46 percent
7. –> Not specified – (lines 143-144) – 41 percent
8. –> Not specified – NA – 37 percent
9. –> Yes – lines 159-166 – 75 percent

The Correct Answers

1. –> Not specified – NA – 25 percent
2. –> Yes – lines 32-33, 78-79, 81-83, 74 – 97 percent
3. –> No – lines 112-122 – 25 percent
4. –> Yes – lines 103-106 – 87 percent
5. –> Yes – lines 113-122 - 75 percent
6. –> Not specified – (lines 159-156) – 46 percent
7. –> Not specified – (lines 143-144) – 41 percent
8. –> Not specified – NA – 37 percent
9. –> Yes – lines 159-166 – 75 percent
10. –> Not specified –NA – 26 percent

Understanding ‘Consent’

Understanding consent

- What is consent?
  - Voluntary agreement to a proposal
  - Contract Act, 1872
    - agreement to the same thing in the same sense
    - "free consent" - no fraud, misrepresentation, coercion, undue influence, mistake.
  - Consent can be express or implied
- Why is consent important?
  - Forms the basis for collection and processing of personal data in many jurisdictions
  - Rooted in the normative value of individual autonomy that is the cornerstone of modern liberal democracies

Privacy as Control

- Consent –> Enables individuals to control their information / identities
- Per Sanjay Kishan Kaul in *Puttaswamy* (2017) - *"Every individual should have a* ***right to be able to exercise control over his/her own life and image*** *as portrayed to the world and to control commercial use of his/her identity. This also means that an individual may be permitted to prevent others from using his image, name and other aspects of his/her personal life and identity for commercial purposes without his/her consent."*

The problem with consent

Growing concern that consent is broken

- People don't read privacy policies
- Consent fatigue
- Unrealistic to expect assessment of downstream use and transfer of data.
- Complex privacy harms (such as discrimination) are difficult to foresee
- Choices are often binary - opt-in or opt-out

Disclosures in Privacy Policies: Does Notice and Consent Work?

Objective

- Is consent broken because of the way policies are currently designed?

Objective

- Is consent broken because of the way policies are currently designed?
- What are we evaluating?
  - **Accessibility and quality of privacy policies** (pre GDPR version) of 5 online services
    1. WhatsApp
    2. Google
    3. Uber
    4. Flipkart
    5. Paytm
  - **Survey to assess intelligibility** - how much do users typically understand of what they sign up for?

Analysing privacy policies

Criteria for assessment

- Access to privacy policies:
  - *Number of clicks to access*: The further embedded a policy is, more time and patience it requires.
  - *Length of the policy*: Longer the policy, the more challenging it may be to read.
  - *Number of (Indian) languages the policy is available in*: Less than a quarter of Indians speak English as their first language.
  - *Readability*: Flesch-Kincaid reading level tests
  - *Language*: Ambiguous or vague terminology
- Visual presentation: use of highlights, section notes etc.
- Substantive content of the policy: Clear and specific provisions on accepted privacy principles.

Access to the policies

Service	(1) No. of clicks	(2) Length	(3)	(4) Language	(5) Readability
		Pages (A4)	Words		Reading ease
Uber	2	11	3,355	Eng.	16.44
WhatsApp	2	10	3,352	Eng.	36.56
Google	1	9	2,890	Eng., Ind.	18.30
Flipkart	1	5	1,767	Eng.	41.03
Paytm	3	3	819	Eng.	20.55

- At least 1-3 clicks away.
- Indian policies are shorter - but perhaps because they cover fewer issues.
- Only Google provides the privacy policy in Indian languages
- Reading ease translates to college or university level.
- Require reasonably advanced comprehension

Visual presentation

- Multiple sections with headings in bold font (Uber, Google, WhatsApp)
- Notes to summarise each section making it easier to understand at a glance (Uber)
- Additional pop-ups when a user moves the cursor (Google)
- Separate overview page (Uber)
- Click-throughs for more information (Uber, Google)

Ambiguous terminology

- Policies do not have a "definitions" section (except for Google) - terms are undefined, or users have to locate them elsewhere.
- "We do not retain your messages in the ordinary course of providing our services to you"
- "We do not share data with third parties but may share with affiliates"
- "We collect device specific information when you install, access, or use our Services. This includes information such as hardware model, operating system information, browser information...."

Ten recognised principles of data privacy

1: Collection
2: Permitted use
3: Sharing with third party
4: Use by affiliated entities
5: Sharing with government
6: Data breach notification
7: Access to own data
8: Data retention
9: Seek clarification
10: Exporting of data

Overview of substantive analysis

- All policies enable collection of large quantities of personal data.
- Various rights considered essential in modern privacy law are not included, relevant information not always provided (eg: data breach notification, data retention, data portability - except google, identity of processor, place where data is processed, etc.)
- MNCs provide some information on access and correction rights
- Flipkart has the highest number of unspecified issues
- All policies have some information on data sharing practices.
- No mention of technical tools other than cookies (except for Google)

Survey: How much do users understand?

Methodology for the pilot

- **Target group:**
  - Read and understand English
  - College education
  - Familiarity with selected services
  - Law and non law background

Methodology for the pilot

- **Target group:**
  - Read and understand English
  - College education
  - Familiarity with selected services
  - Law and non law background
- **Three kinds of questions:** 1) Easy; 2) Intermediate; 3) Difficult

Methodology for the pilot

- **Target group:**
  - Read and understand English
  - College education
  - Familiarity with selected services
  - Law and non law background
- **Three kinds of questions:** 1) Easy; 2) Intermediate; 3) Difficult
- **Possible responses:** 1) Yes; 2) No; 3) Not specified; 4) Can't say

The classification

Q1: Collection	Easy
Q2: Permitted use	Intermediate
Q3: Sharing with third party	Difficult
Q4: Use by affiliated entities	Intermediate
Q5: Sharing with government	Easy
Q6: Data breach notification	Difficult
Q7: Access to own data	Difficult
Q8: Data retention	Intermediate
Q9: Right to seek clarification	Easy
Q10: Exporting of data	Difficult

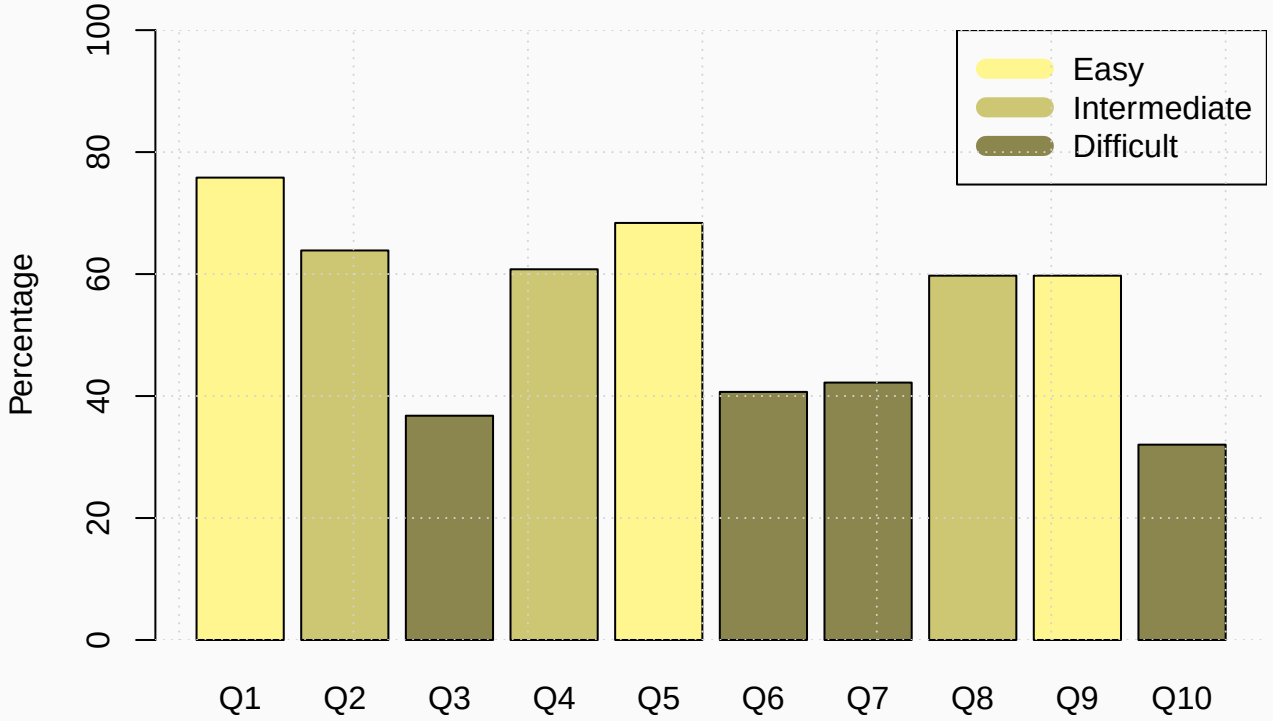
The sample

- 155 respondents across colleges/universities in Delhi.
- 33% (N=51) with law background, 67% (N=104) with non-law (economics and managements) background
- 59% (N=92) post-grad students, 41% (N=63) under-grad students
- Responses distributed across policies as follows:
  - Flipkart: 21% (N=32)
  - Google: 21% (N=33)
  - Paytm: 24% (N=37)
  - Uber: 10% (N=16)
  - WhatsApp: 24% (N=37)
- Respondents took between 10-20 minutes to fill up the forms.

Average scores

	Average Score
Overall average	5.30
By policy	
Flipkart	5.31
Google	5.36
Paytm	5.54
Uber	5.88
WhatsApp	4.65
By study area	
Non-law	5.3
Law	5.2
By degree	
Under graduate	5.1
Post graduate	5.3

Correct responses by question



- More than 60% of respondents answered the easy questions correctly.
- The least correct respondents were for the difficult questions, followed by the intermediate ones.
- Therefore, when a policy has complex terminology or ambiguous terms, user understanding correspondingly decreases

How many people answered can't say

One metric of understanding is to not be saying "can't say".
Average score on "can't say" by policy:

- Flipkart: 0.71
- Google: 1.18
- Paytm: 0.81
- Uber: 0.93
- WhatsApp: 0.76

Google has the most detailed policy but does that increase complexity?

Conclusions from the paper

- Complex factors at play - length of policy; clarity of legal terms; ex-ante perceptions of respondents
- Policies are primarily written to address legal requirements and avoid liability claims
- Policies assume that the user has a knowledge of legal terms and regulatory requirements
- When specific features are "not specified", they lead to poor understanding.
- Legal terms such as "third-party" and "affiliate" are confusing, and inhibit understanding.

The draft Personal Data Protection Bill, 2018: Notice and Consent

How do you solve the problems with notice-consent?

- Shift focus from consent to accountability?
- Ways to make consent more meaningful?
- Srikrishna Committee Report and the draft PDP Bill tries to do both.

Key terms in the draft PDP Bill, 2018

- "personal data" - Section 2(29)
- "sensitive personal data" - Section 2(35)
- "data principal" - Section 2(14)
- "data fiduciary" - Section 2(13)
- every processing has to have a valid ground (basis)

Notice - Section 8, draft PDP Bill, 2018

- Information to be provided at the time of collection or as soon as reasonably possible (if data collected from third parties).

Notice - Section 8, draft PDP Bill, 2018

- Information to be provided at the time of collection or as soon as reasonably possible (if data collected from third parties).
- Information to be provided in a clear, concise manner that is comprehensible to a reasonable person

Notice - Section 8, draft PDP Bill, 2018

- Information to be provided at the time of collection or as soon as reasonably possible (if data collected from third parties).
- Information to be provided in a clear, concise manner that is comprehensible to a reasonable person
- Information to be provided in multiple languages where necessary and practicable

Information required in a notice

- purposes for which the personal data is to be processed
- categories of personal data being collected
- identity and contact details of the data fiduciary, data protection officer, grievance redress mechanism
- rights to withdraw consent, procedure for such withdrawal personal data
- whom the data will be shared with
- information regarding cross-border transfers of data
- period for retention
- existence and procedure for exercising user rights (correction, access, etc)
- data trust scores

Grounds for Processing of Personal Data

- Consent (S 12)
- State function authorised by law (S 13)
- Compliance with law or court order (S 14)
- Processing for prompt action (S 15)
- Processing for purposes related to employment (S 16)
- For reasonable purposes (S 17)

Consent: Section 12

- *When?* No later than at the time of commencement of processing

Consent: Section 12

- *When?* No later than at the time of commencement of processing
- Conditions for valid consent:
  - Free - i.e. no coercion, misrepresentation, fraud, mistake, undue influence
  - Informed - Notice requirement is fulfilled
  - Specific - scope of consent to be determinable
  - Clear - meaningful affirmative action
  - Revocable - ease of withdrawal to be comparable to ease of consenting

Consent: Section 12

- *When?* No later than at the time of commencement of processing
- Conditions for valid consent:
  - Free - i.e. no coercion, misrepresentation, fraud, mistake, undue influence
  - Informed - Notice requirement is fulfilled
  - Specific - scope of consent to be determinable
  - Clear - meaningful affirmative action
  - Revocable - ease of withdrawal to be comparable to ease of consenting
- Provision of goods/services cannot be tied to consent for processing of unconnected data
- Consent must be verifiable

Grounds for Processing of Sensitive Personal Data

- Explicit consent (S 18): *more information, more clarity, more specificity* –> higher standard than for personal data
- Where strictly necessary for certain state functions (S 19)
- Compliance with law or court order (S 20)
- Processing for prompt action (S 21)

Some examples:

- *An airport screens passengers before they are allowed to board a plane, using body scanners. Can it rely on consent/explicit consent as a ground for processing?*

Some examples:

- *An airport screens passengers before they are allowed to board a plane, using body scanners. Can it rely on consent/explicit consent as a ground for processing?*
- **Answer:** No free consent, as no real choice –> need to use another ground, such as a specific law or state interest (EU Commission Regulation No. 1141/2011)
- *An airline transfers passenger records, eating habits of the customer, and health problems to immigration authorities in a foreign country. Can they use consent/explicit consent as a valid ground for processing?*

Some examples:

- *An airport screens passengers before they are allowed to board a plane, using body scanners. Can it rely on consent/explicit consent as a ground for processing?*
- **Answer:** No free consent, as no real choice –> need to use another ground, such as a specific law or state interest (EU Commission Regulation No. 1141/2011)
- *An airline transfers passenger records, eating habits of the customer, and health problems to immigration authorities in a foreign country. Can they use consent/explicit consent as a valid ground for processing?*
- **Answer:** No free consent, as no real choice if you want to enter the foreign country –>need to use another ground such as a specific law (Council of EU, Handbook on Data Protection Law)

Some more examples:

- *An online store collectes personal details of a customer when they order some goods. At the time of checking out, the customer is asked to check a box allowing their data to be processed by the store and for their data to be passed onto third party partners of the online store - who will use the data for marketing. Is the consent valid?*

Some more examples:

- *An online store collectes personal details of a customer when they order some goods. At the time of checking out, the customer is asked to check a box allowing their data to be processed by the store and for their data to be passed onto third party partners of the online store - who will use the data for marketing. Is the consent valid?*
- **Answer:** No - the online store is making sharing the data with their partners a condition of the sale when not necessary (to process the order/deliver the goods). Consent is not specific and freely given.
- **Remedy** –> the company should provide an additional opt in for the sharing of the data. (ICO, UK)

Some more examples (contd.):

- *A spa gives a form to its customers that states: "Skin type and details of any skin conditions (optional): / We will use this information to recommend appropriate beauty products." Is this explicit consent?*

Some more examples (contd.):

- *A spa gives a form to its customers that states: "Skin type and details of any skin conditions (optional): / We will use this information to recommend appropriate beauty products." Is this explicit consent?*
- **Answer:** This is implied consent (despite the consent freely given, specific, informed and with an unambiguous affirmative act.)
- **Remedy** –> Add a checkbox with the statement "I consent to you using this information to recommend appropriate beauty products." (ICO, UK)

Processing of Personal Data of Children

- Consent of child does not constitute valid consent
- S. 23 - appropriate age verification mechanisms to be implemented + mechanisms for parental consent

Miscellaneous provisions

- S 41 - Consent to transfer data abroad (as an exception to the general rule)
- S. 92 - Explicit consent required to de-anonymise data

Effects of withdrawing consent for processing

- Requirement to delete / anonymise personal data
- Data fiduciary can stop providing the relevant service - but not unconnected services.

Summarizing consent in the PDP Bill, 2018

- Relatively high standard of consent in the draft PDP Bill
- Valid consent to process personal data must be free, specific, informed, clear and specific
- Higher standard for sensitive personal data - explicit consent
- There are also various grounds for non-consensual processing
- PDP Bill puts in place a series of user rights / data fiduciary obligations that apply across the board
- Overall requirement to process data fairly and reasonably.

Improving Notice and Consent

Suggestions of the JSK Committee

- **Model forms for notice:** Compliance means no liability on this ground for data fiduciaries, easier understandability for users. But will forms be sufficient, well-designed and up to date?
- **Data trust scores:** Labelling systems, easy for users to understand how safe their data is.
- **Dynamic consent:** Single place to control all personal data, ability to change settings at all times. Eg: Privacy dashboards

Improving Notice

- Policies in local languages where service is available
- Simplify text
- Provide collapsible sections, with clearly distinguished topics
- Use pop-ups and layered notices
- Use section summaries, colours and icons where possible
- De-bundle permissions and ensure no use of opt-outs
- Use legible fonts, proper spacing and pagination, visual markers
- Use non-written methods where possible (Eg: video clips to explain concepts)

Looking ahead:

- AI to enhance explainability: Eg - Pribot/Polisis

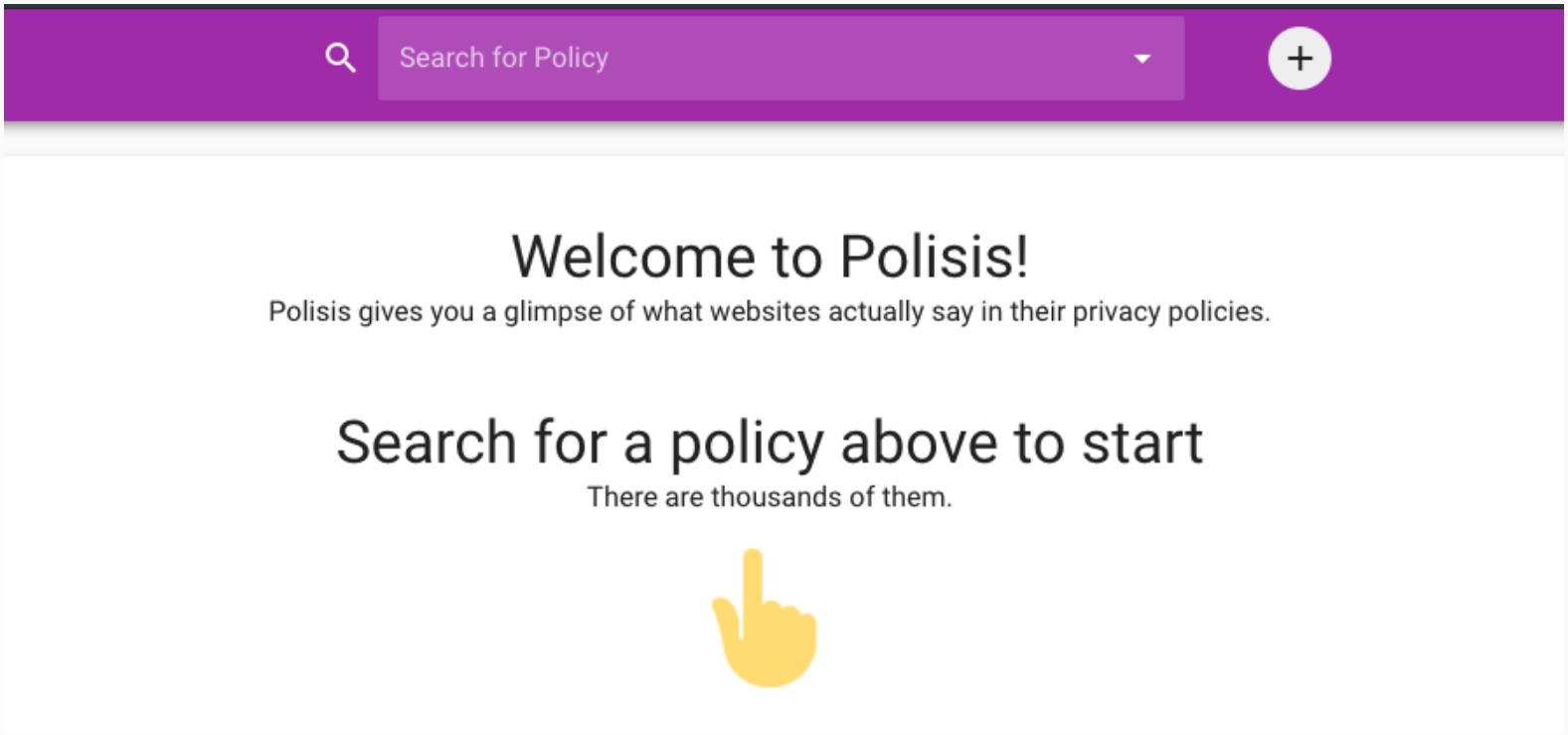
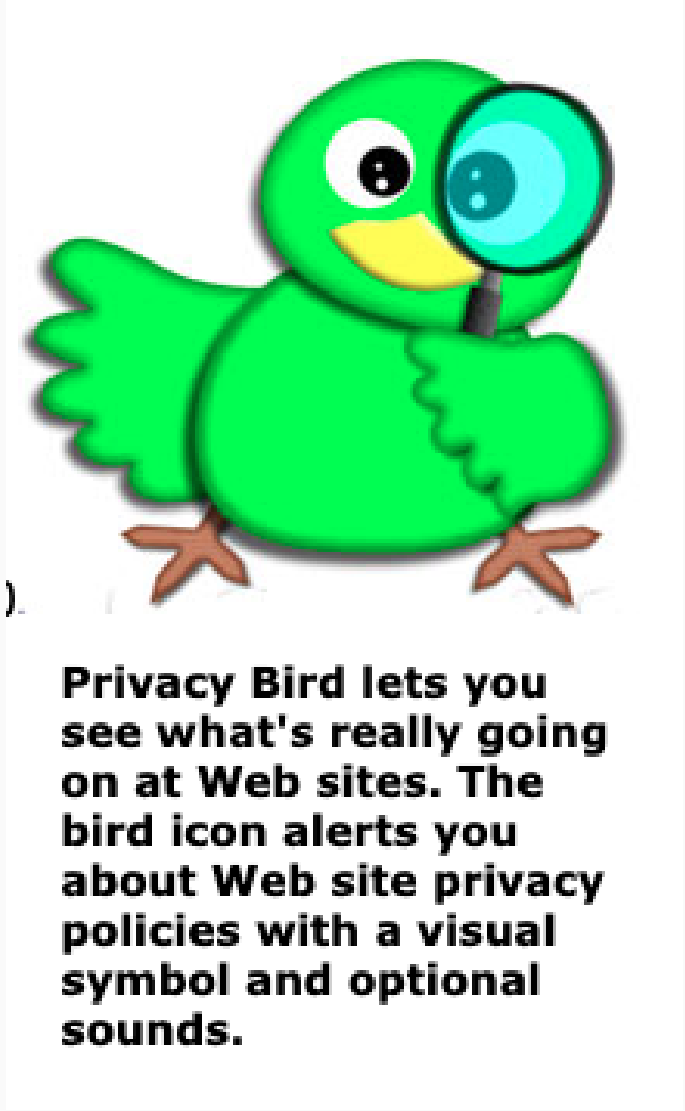


Figure 1: Pribot

Looking ahead:

- Software to alert users: Eg - Privacy bird



Conclusions

Conclusions

- Consent is seen as providing autonomy to the individual
- There are numerous problems with the notice-consent framework as it exists today
- The draft PDP Bill tries to solve some of these by ensuring a relatively high standard for providing notice and securing consent of users.
- Further, all processing under the draft law has to be "fair and reasonable" + comply with the various rights / obligations provided for in the law.

Comments/Questions?

Thank you