Why Johnny Can't Encrypt

- Paper Hypothesis: effective security requires a different usability standard, and that it will not be achieved through the user interface design techniques appropriate to other types of consumer software

- User errors contribute the most to security failures
    a. Security needs to be made more manageable and user-friendly as many novices are having to make use of network devices for private transactions
    b. Legal remedies, automation, user training are temporary fixes or solutions
    c. Ultimately UI design problem
    d. Regular UI standards for consumer software do not apply to security
- Security software is usable if the people who are expected to use it:
    a. are reliably made aware of the security tasks they need to perform
    b. are able to figure out how to successfully perform those tasks
    c. don't make dangerous errors
    d. are sufficiently comfortable with the interface to continue using it.
- They employ two methods for evaluating the usability of PGP: cognitive walkthrough and lab user test.
- Properties of security to be taken into account while designing interface that make it different from regular consumer software
    a. Unmotivated user: User places more importance on using the primary feature (sending email). Security is secondary and/or assumed to be working fine. Do not assume users will read manual about security.
    b. Abstraction: Security policies are abstractions that users may not know about (like me)
    c. Lack of feedback: You cannot get feedback reliably about security software as systems are complex and user knows what is the best security config they want so hard to perform check.
    d. Barn door: Make user understand security v well to prevent high-cost mistakes
    e. Weakest link: Make user aware of all aspects of security (v similar to above)
- Usability standard for PGP. User should:
    a. Understand privacy is achieved through encryption. Be able to encrypt and decrypt email (UNDERSTAND PUBLIC KEY MODEL)
    b. Understand auth is achieved through signatures. Be able to sign and verify email. (UNDERSTAND PUBLIC KEY MODEL)
    c. Understand exactly how the above two can be done (explained thoroughly in paper) (HOW TO ACHIEVE)
    d. Not make fatal errors like: sending email without encryption, trusting wrong public keys, failing to back up private keys, forgetting passphrases (IRREVERSIBLE ACTIONS)
    e. Succeed within few hours of reasonable effort

- Evaluation Methods
    a. Cognitive walkthrough
        - Similar to code walkthrough, mentally dry run the software as a novice user
        - They employed aspects of heuristic evaluation - evaluated UI against high-priority usability principles.
        - Double experts perform this - experts in domain as well as its usability by the commonfolk
    b. User test / Lab test
        - Two challenges
            - We must tell them what the basic requirement is from the user of the software to get them started which conflicts with the goal of providing awareness about the requirement through the software itself
            - We must give user something they would want to protect in real-life to make sure the test is carried out fairly

- Cognitive Walkthrough
    - Visual Metaphors
        - Keys: better icons
        - Signatures: better icons
    - Different Key Types
        - New version of PGP uses Diffie-Hellman/DSS while old ones use RSA
        - Not explained well in UI
    - Key Server
        - “Key Server” menu instead of “Keys” menu to give user better understanding that they are connecting to a remote
        - Key revocation certificate publicization should be prompted (as it doesnt happen automatically)
    - Key Management Policy
        - Trust and validity ratings meanings must be made more clear to user
    - Irreversible Actions
        - Failing to encrypt
        - Deleting private key
        - Publishing key to server
        - Revoking key
        - Forgetting Passphrase
        - Failing to backup keyrings
    - Consistency
        - “encoding” is used in the software instead of “encrypting”
    - Too Much Information
        - Have clear distinction between beginner and advanced features in UI (eg: trust and validity labels)

- User Test
    - Following tasks were evaluated:
        - Avoiding dangerous errors, figuring encrypting, figuring correct key to encrypt, decrypting, publishing public key to server, getting others' public keys, mixed key types, signing, verification
- Conclusion
    - Despite the UI being attractive, and easy to understand for experienced user, novice users faced the following problems
        - Could not figure out public key model
        - If figured model, going about tasks was tough
        - Could not encrypt
        - Experienced frustration in using the software
    - Better design strategy
        - Short, concise, conceptual model of security software must be established
        - Model must be communicated effectively to user
        - More accurate metaphors needed

Imagined Communities: Awareness, Information Sharing, and Privacy on the Facebook

- look for underlying demographic or behavioral differences between the communities of the network's members and non-members
- Find patterns and motivations in the information revelation of students
- analyze the impact of privacy concerns on members' behavior
- we compare members' stated attitudes with actual behavior
- document the changes in behavior subsequent to privacy-related information exposure

Elementary Results:

- Privacy concerns do not stop people from using FB
- People are unaware of the size of the online community and the visibility of their profile
- Concerned individuals also reveal great amounts of info, small fraction of them use privacy settings to reduce revelation of information

Non members of social media (like your employer) might use social media to get information on you which you have provided on such sites. Changing trends, more familiarity with new technology, lack of info about misuse of personal information encourage people to reveal information on these websites. Platforms making it easy to add personal information and reducing costs of storing and mining such information has sped up information collection as long as there is the incentive to store this data somewhere.

FB is of interest to researchers in two respects:

1) as a mass social phenomenon in itself
2) patterns of privacy concern and info reveal by people
3) they show personal info (like contact no) usually not present on other social media

Results

Privacy Attitudes
Three types of Qs were asked on a 7 point likert scale. Privacy questions were interspersed with other questions for a baseline and also to prevent the taker from learning via the survey.

1. General : How important is x in public debate
2. Specific : How imp is x for you on day to day basis
3. Personal : How worried will you be if x happens

In case of personal questions, privacy was given highest worry but in others educational policy etc were first. Non members showed more concern for privacy than members. This does not mean privacy concerns reduce chances of joining fb, users with highest privacy concerns are also fb members. In their model, age and being a ug student were imp features to determine chances of joining fb.

Information Provision
Females less likely to give sexual orientation or phone number, but have similar stats for other info.
If anything, we found new confirmations of a privacy attitude/behavior dichotomy. Almost 16% of respondents who expressed the highest concern (7 on the Likert scale) for the scenario in which a stranger knew their schedule of classes and where they lived, provide nevertheless both pieces of information (in fact, almost 22% provide at least their address, and almost 40% provide their schedule of classes)

Awareness of Facebook Rules and Profile Visibility
The majority of FB members claim to know about ways to control visibility and searchability of their profiles, but a significant minority of members are unaware of those tools and options. Most people are aware that millions can see their profile but are not concerned about this. People share information on facebook so that people can find them or to have fun but there are psychological implications behind it, people tend to be concerned about others revealing information but not about themselves. As a result of learning from the survey, few people who demonstrated high privacy concerns changed the privacy settings of their profiles.

Evaluating the Contextual Integrity of Privacy Regulation: Parents' IoT Toy Privacy Norms Versus COPPA

Intro: Increase in privacy concerns has increased regulations regarding protection of data (protect sensitive personal data from unauthorized use or release) across the world. It is important to determine whether these **regulations align with the privacy norms** of the people concerned. They develop a surrey model based on **contextual integrity** (*theory of information privacy which argues that social relations are guided by norms in information flows and that privacy is violated when these norms are violated.)* This survey can be applied to regulations dealing with **data transfer** and **collection**.

- Covers concrete privacy scenarios that can be understood by people from different backgrounds.
- It uses longitudinal (several points in time) and cross section (several samples in one time) measurements to keep track of effectiveness of regulation updates over time.
- Provides the first quantitative evidence that COPPA's restrictions on smart toy data collection generally align with parents' privacy expectations.

Contextual Integrity describes information flows using 5 parameters:

1. Subject of transferred information us
2. Sender of information (us)
3. Attribute or type of information (Browsing history)
4. Recipient of information (Search Engine)
5. Transmission principle (condition imposed on transfer) (To Improve search results, notification will be provided, etc)

We can determine the privacy norms of the parents by obtaining how appropriate and accessible they find Information flows with different combinations of these five principles determined.

Working of survey method

1. A combination of the 5 attributes is chosen based on some particular privacy regulation. We create information flows which can be allowed or disallowed by this regulation.
2. Survey respondents rate their acceptability of the above generated information flow. It is ensured that each flow is a concrete data collection scenario and is understandable.
3. Average acceptability of the flows allowed or disallowed by this regulation determines if it conforms to the norms of the ppl. Variations indicate there might be parts of the regulation for some particular information flow or demographic indicates some privacy norms might not align with the regulation.

Some Examples for each Parameter used in the survey :

1. Transmission principle : Whether parents can give consent, review information, revoke consent, storage, deletion, whether it complies with coppa, null.

2. Attributes: Location, sleep time, frequency of use, heart rate, audio, video, bday
3. Recipients : Manufacturers, third party service providers
4. Subject is always the child
5. Sender is the smart toy

Survey Overview

- **Consent**
- **Demographic :** Age of children (<13)
- **Overview:** Chose one child age , and brief description on devices and instructions.
- **Contextual Integrity Questions:** Core of the survey consisted of 32 blocks of questions querying the acceptability of our generated information flows . Each question block contained 33 information flows with the same sender, same attribute, varying recipients, and varying transmission principles. This reduced cognitive fatigue and added emphasis on transmission principle. Each individual multiple choice question in the matrices asked respondents to rate the acceptability of a single information flow on a scale of five Likert items. *Each question block also included one attention check question.*
- **Awareness Questions**
- **Demographic Questions :** Standard demographic questions

The results were analyzed in different groups for statistical measures. Groups were

- Subject and Attribute
- Demography based groups (COPPA familiarity, age, smart device ownership, education, and income)
- Recipient
- Sender (device)

Across transmission principles broadly classified into

- Notification and consent (perms asked)
- Confidentiality & Security (can be deleted)
- COPPA Compliance (compliant with coppa)
- Coppa exclusions (device needs for functioning)
- null

Results:

- **Overall, surveyed parents view information flows meeting COPPA data collection guidelines as acceptable while viewing equivalent information flows without COPPA criteria (null) as unacceptable . This supports the conclusion that COPPA-mandated information handling practices generally align with parents' privacy norms.**
- **Information flows with the transmission principle "if the information is used to serve contextual ads" have negative average acceptability scores across almost all senders, recipients, and attributes . Unlike all other information flows on our**

survey with non-null transmission principles, these flows are actually prohibited by COPPA.

- **Parents gave low scores with attribute of child's birthday, can be due to smaller percentage of ppl given this attribute or because they found it irrelevant to the principal**
- **transmission principles in the notification/consent category have significantly higher acceptability scores than flows with transmission principles in the confidentiality/ security category by an average of 0:43 Likert scale points. This indicates prioritization of consent over security.** ***One notable exception to this trend is the transmission principle "if its privacy policy permits it" which is low for notification/consent category. This indicates distrust in general privacy policies.***
- **Information flows with the transmission principle "if it complies with the Children's Online Privacy Protection Rule" received a positive average acceptability score of 0.49 across all senders, recipients, and attributes. People more familiar with COPAA were more accepting.**
- **Younger Parents are More Accepting of Smart Toy Data Collection**
- **Parents Who Own Smart Devices are More Accepting of Data Collection**
- **Unexpected Result: Education & Income have Little Effect on Parents' Smart Toy Privacy Norms**

Limitations

1. Privacy behavior different from privacy reporting on surveys
2. Demographic Biased , more women , only USA

Applications

1. The CI survey method could also be incorporated into the policymaking process
2. Policymakers could test whether previous regulatory approaches will be applicable to new innovations by conducting surveys with CI parameters describing new technologies and existing regulation
3. Can be used by manufacturers to see which norm they will violate

Conclusion

We find that information flows conditionally allowed by COPPA are generally viewed as acceptable by the surveyed parents, in contrast to identical flows without COPPA mandated restrictions. These are the first data indicating the general alignment of COPPA to parents' privacy norms for smart toys. However, variations in information flow acceptability across smart toys, information types, and respondent demographics emphasize the importance of detailed contextual factors to privacy norms and motivate further study.

Privacy Wizards for Social Networking Sites

Real users conceive their privacy preferences (which friends should be able to see which information) based on an implicit set of rules. Thus, with a limited amount of user input, it is usually possible to build a machine learning model that concisely describes a particular user's preferences, and then use this model to configure the user's privacy settings automatically. It is based on uncertainty sampling, the user selects informative friends and it uses this data to get uninformed friends. Users define their informed friends based on communities, and using these as features we can determine the privacy settings. On average, if a user labels just 25 (of over 200) friends, the wizard configures the user's settings with > 90% accuracy.

It has an advanced section for advanced users to modify the settings and visualize the process.

- Visualization : Shows nodes (each node denotes a common aspect) between people like a decision tree along with info of labeled friends and how many friends are in this node)

Second, we observed that in some cases the resulting decision trees are large, and difficult to view all at once. To help guide users towards parts of the tree that are likely to require attention, we incorporate two additional pieces of information for each node:
• **Class Distribution:** For each node in the tree, the visualization indicates the class distribution (i.e., proportion labeled allow and deny) of the labeled friends who satisfy the conditions for the (subtree rooted at the) node.
• **Representative Rate:** the proportion of labeled friends among all friends who satisfy the conditions for a node.

- Modification : Allows users to label more people in that node

Challenges

1. Low effort high Accuracy: users have trouble with privacy and security policies hence input should take low effort from the users.
2. Graceful Degradation : More input means more accuracy, but should not rely on more input.
3. Visible Data : Should use input + data visible to U as a user.
4. Incrementality : Settings should evolve as more friends added

Framework
Essentially is a binary classifier for <friend, data item> pairs.

1. User Input: Questions about privacy preferences, user can quit any time (Active learning)
2. Feature Extraction: Using the information visible to the user, the wizard selects a feature space ~X . Each of the user's friends can be described using a feature vector ~x in this space.
   The features are
   - **Communities** : For each community and friend, 0/1 value. Use edge betweenness algo to maximize modularity
   - Other Profile features: Personal info (**profile info**), fan pages, tagged pics (**online activities**) etc
3. Privacy-Preference Model : Constructs the actual model

Uncertainty Sampling

- In the sampling phase the wizard asks the users to label friends. Initially all unlabelled, then asks for the labels of k most uncertain friends. Repeats till the user quits.
- Classifier Construction Phase generated the predictions for the unlabelled friends.

Evaluation

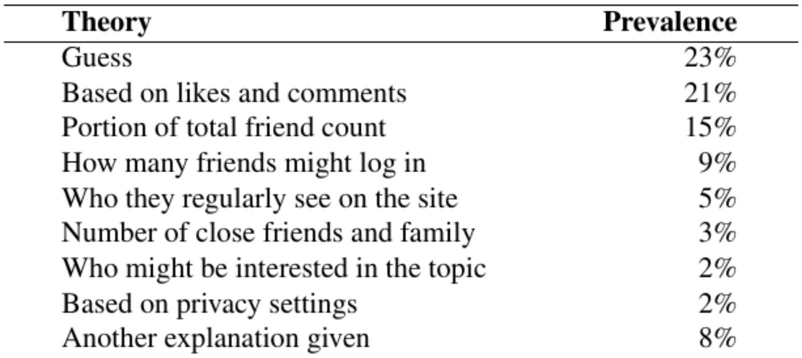
- Two questionnaires, one general (some all none) and one detailed (for “some” case, which?) were conducted. Different classifiers such as (Decision Tree, Brute Force, DTree Active) were compared based on accuracy of labeling. Even features were compared, and using communities was the best, profiles and fan pages did not add much.

answer the following two questions:
• How effective is the active learning wizard, compared to alternative policy-specification tools?
• Which features (e.g., community structure, profile information, etc.) are the most useful for predicting privacy preferences?

Quantifying the Invisible Audience in Social Networks

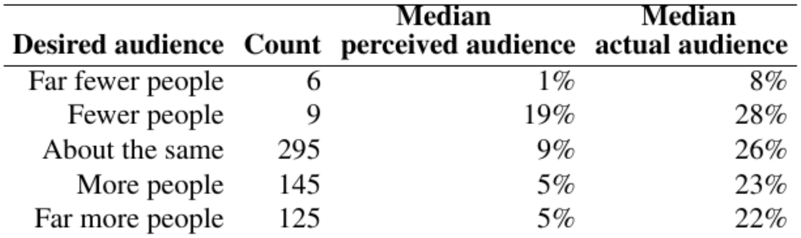
- Introduction
  - Visible participation in social media: comments, likes
  - Invisible participation is difficult to know (duh)
    - However users do have a mental model of who is viewing their content
    - Good: provides plausible deniability to audience
    - Bad: Knowing exactly who is viewing our posts affects the way we act. OP should be allowed to make informed decisions about our privacy.
    - Folk theories used by users to guess (more on this later)
  - Researchers survey users to get their estimate on the invisible participation and compare it with their data from server logs (*)
  - Are friend count, feedback good heuristics to estimate actual audience? (*)
- Related Work
  - Peace maaro
- Method and Data
  - They focus on the contexts where intended audience is the friends of the user
  - Audience logs
    - Tracked posts of randomly chosen 220000 users
    - If post appeared on a user’s viewport for non-trivial amount of time, logged
    - Feedback in the form of likes and comments were logged
  - Survey
    - Two types of surveys conducted to know what the users think their audience count is (perceived audience)
    - General survey

            - How many people do you think usually see the content you share on Facebook?
        - Specific survey (for specific post made in the last 48 hrs)
            - How many people do you think saw it?
        - Users shared their desired audience size (through a likert scale). So there are three things - perceived, desired and actual audience size.
- **Audience Size Perception**
    - Perception about audience size vs reality:
        - General: 50 median, Specific: 20 median
        - Actual General: 3x perception, Actual Specific: 4x perception
        - General audience size larger than specific post audience size. Makes sense since there might be diff subsets of people viewing diff posts and their cumulative is more than specific
    - Folk theories of users about audience size (heuristics)
        - Participants most often used heuristics based on feedback and friend count
        - Users said stuff like "No of seen will be X times no. of comments/likes"
        - Compared the audience estimation accuracy of each group. Despite the variety of theories of audience size, no theory performed better than users who responded "guess"



Theory	Prevalence
Guess	23%
Based on likes and comments	21%
Portion of total friend count	15%
How many friends might log in	9%
Who they regularly see on the site	5%
Number of close friends and family	3%
Who might be interested in the topic	2%
Based on privacy settings	2%
Another explanation given	8%

    - Perception about audience size vs desire
        - Only 3% of the participants desired a smaller audience than their perception
        - Those who wanted a larger audience (roughly 50% ppl) had made a smaller estimation



Desired audience	Count	Median perceived audience	Median actual audience
Far fewer people	6	1%	8%
Fewer people	9	19%	28%
About the same	295	9%	26%
More people	145	5%	23%
Far more people	125	5%	22%

- **Uncertainty in actual audience size**

    - Friend Count: Post produced by a user with many friends has more variability in the audience size than one produced by a user with few friends.
    - Feedback: Says nothing about audience size, highly variable
    - Joint (both the two): Says nothing
    - These results suggest that audience size can be quite unpredictable
    - Users do not receive enough feedback (aka in the form of likes/comments) to predict their audience size well.
- Reason for audience mismatch
    - Users overestimate friends liking/commenting on posts
    - Users feel more comfortable making smaller estimate coz they would be sad if more people saw it but still did not engage (comment/like)
        - Can be somewhat validated by the fact that general audience estimate was 50 but specific was 20
- Limitations
    - Precision-recall tradeoff in log data collection
    - See != focussing attention on post
    - One-month data may not have external validity
    - Participants may have filtered out people who didnt pay attention to posts while giving their estimate on survey (was not needed)
    - Interviews might have given more in-depth perceptions of users
    - Sampling bias: sampling only active users for both logging + survey
- Design Implications
    - Should we show actual audience size in social media
        - Bad: No plausible deniability for audience, sharers may be disappointed to know abt lack of engagement
        - Good: Knowing that they have larger audience, some users may be more motivated to participate and post content
    - Can show cumulative views on posts over a long period of time (e.g.: in the last 6 months your posts got so and so views)
- Conclusion
    - Users underestimate their audience by a factor of 4 (for specific posts, but generally it is 3)
    - Many users who want a larger audience already have a larger audience than they estimate (desired > perceived but actual >> perceived :clown:)
    - However, the actual audience cannot be predicted in any straightforward way by the user from visible cues such as likes, comments, or friend count.

bottomline: USERS DO NOT RECEIVE ENOUGH FEEDBACK TO PREDICT THEIR AUDIENCE SIZE ACCURATELY.