CSC 495.002 – Lecture 15
Misc Topics

Dr. Özgür Kafalı

North Carolina State University
Department of Computer Science

Fall 2017

Privacy Perceptions

- Westin Categories

- Cultural Studies

- Facebook Studies

- Mental Models

NC STATE UNIVERSITY

What You Will Learn

- Privacy measurement

- App permissions

- Privacy requirements engineering

NC STATE UNIVERSITY

TECHNIQUES & STUDIES

Indirect Content Privacy Surveys

Indirect Content Privacy Surveys: Measuring Privacy Without Asking About It

Alex Braunstein[*]
Chomp
thestatistician@gmail.com

Laura Granka
Google
granka@google.com

Jessica Staddon
Google
staddon@google.com

ABSTRACT

The strong emotional reaction elicited by privacy issues is well documented (e.g., [12, 8]). The emotional aspect of privacy makes it difficult to evaluate privacy concern, and directly asking about a privacy issue may result in an emotional reaction and a biased response. This effect may be partly responsible for the dramatic privacy concern ratings coming from recent surveys, ratings that often seem to be at odds with user behavior. In this paper we propose indirect techniques for measuring content privacy concerns through surveys, thus hopefully diminishing any emotional response. We present a design for indirect surveys and test the design's use as (1) a means to measure relative privacy concerns across content types, (2) a tool for predicting unwillingness to share content (a possible indicator of privacy concern), and (3) a gauge for two underlying dimensions of privacy – content importance and the willingness to share content. Our evaluation consists of 3 surveys, taken by 200 users each, in which privacy is never asked about directly, but privacy warnings are issued with increasing escalation in the instructions and individual question-wording. We demonstrate that this escalation results in *statistically and practically significant differences* in responses to individual questions. In addition, we compare results against a direct privacy survey and show that rankings of privacy concerns are increasingly preserved as privacy language increases in the indirect surveys, thus indicating our mapping of the indirect questions to privacy ratings is accurately reflecting privacy concerns.

1. INTRODUCTION

Privacy surveys are quite frequent, and the reported results are often dramatic, e.g. more than 70% of users are concerned about online tracking [38] and 93% of users are concerned about company/government access to health records [39]. Almost as frequent though, are reports of consumer behavior that seem incompatible with the high priority on privacy indicated by the surveys. For example, users publicize their purchase histories on web sites like Blippy [4], are willing to trade personal information for entries in sweepstakes or coupons and pay little attention to privacy policies that are reported to be highly valued [16, 15, 18, 35, 9].

We investigate several scenarios in which the mere act of reminding users about general privacy and security issues around content, primes the user. In particular, we study how questions about content use and content importance change when privacy and security language is introduced. As the language escalates, results show increased similarity between responses to our surveys and to a survey that asks about content privacy concerns directly (e.g. "How *private* do you consider this information?").

One explanation for such an effect is education, that is, survey respondents learn, or are reminded, of privacy risk through the survey; thus explaining how behaviors measured elsewhere are inconsistent with survey responses. While some kind of education-effect is likely; it is our belief that it does not account for the bulk of the phenomenon given the high volume of privacy-related news stories in recent years, and the growth of organizations focused on privacy research

Braunstein et al. Indirect content privacy surveys: measuring privacy without asking about it. Symposium on Usable Privacy and Security (SOUPS), pages 15:1–15:14, 2011

Motivation and Objectives

- Problem: Hard to evaluate privacy concerns due to emotional reactions and other biases
- Explicitly mentioning content sensitivity invites exaggerated reporting of privacy concerns

- Explore indirect techniques to diminish emotional responses
- A measure of relative privacy concerns across content types
- A tool for predicting unwillingness to share content
- A gauge for two dimensions of privacy: Content importance and sharing preferences

Study Design

Study	Instructions
1	We are studying the importance of different online information sources in daily life. Please answer a few questions about your use of the given information source or sources.
2	We are studying the importance of different online information sources, many of which are privacy-sensitive and common targets of phishers and others who commit online fraud. Please answer a few questions about your use of the given information source or sources.
3	We are studying the importance of different online information sources, many of which are privacy-sensitive and common targets of phishers and others who commit online fraud. Please answer a few questions about your use of the given information source or sources keeping in mind the potential privacy risks of sharing or otherwise revealing who commit online fraud.

Survey Questions

Number	Question	Answer Options
1	How frequently do you check [content type]?	Several times a day About once a day A few times a week A few times a month A few times a year Almost never
2	How often do you refer to a [content type] that is several weeks old?	Same as above.
3	How frequently do you forward or otherwise share (e.g. by printing and giving the printed copy) [content type] with your close friends or close family members?	Same as above.
4	(Keeping in mind that purchase records may contain sensitive information,) How many of your [content type] would you be willing to show to your close friends and close family members?	All of them The majority of them Some of them Not very many of them None of them
5	(Keeping in mind that purchase records may contain sensitive information,). if you were to leave a hard copy of one of your [content type] on a restaurant table how likely are you to return to retrieve them?	Very Likely Likely Sometimes I would, sometimes I would not Rarely Never
6	Let's say a server went down and you lost access to your [content type] for two weeks. How would this affect you? It would be...	Extremely disruptive Very disruptive Somewhat disruptive Not very disruptive Not disruptive at all
7	Imagine you have lost access to all the following information sources: email, online calendar, online photos, online documents, Web history and online newspaper. That is, you can no longer access old emails, online calendar entries, online photos, online documents, Web history, online bank/credit card statements, and online newspapers or receive/create new instances of any of these. There is a team available to recover these materials for you, and they need to know how to focus their attention. Please rank the information sources in the order in which the team should work on recovering them (with number 1 being the source the team focuses on first).	Ranked ordering of content types

Purpose of Questions

- Questions 1 and 2: Assess frequency of use
- Questions 3 and 4: Strong signals for sharing frequency
- Questions 3 and 5: Both content importance and content visibility
- Question 6: Speaks directly to importance of content
- Question 7: Overt measure of user importance, replicates Question 5

Exercise: Which Content Type to Recover?

- Content types: Email, news, calendar, photos, documents, purchases, bank records, web history

Most frequent Choice For Each Ranking	1	2	3	4	5	6	7	8
Study 1	email	bank/CC	docs	docs	purchases	purchases	Web history	news
Study 2	email	bank/CC	docs	purchases	purchases	photos	news	news
Study 3	email	bank/CC	docs	docs	purchases	Web history	calendar	news

Direct Privacy Survey

- Suppose your computer had a virus that gave it access to ALL of your information on this computer and the Internet. Specifically, it would have access to: email, calendar, photos, documents, contacts, Buzz/Twitter, online purchases, web history.

Limitations and Mitigations

- Self-reporting of behaviors: Build redundancy into the survey
  - Unable to estimate or recall behaviors
  - Social-desirability bias
  - Priming – intentional or unintentional

- Prediction of future behaviors

- Minimize response bias

Content Rankings

content Type	Email	Online Documents	Web History	Online Purchases	Online Photos	Online Calendar
Average Privacy Rating	4.32	4.25	3.87	3.76	3.7	2.62

	Direct Study	Study 3	Study 2	Study 1
1.	email	email	email	email
2.	documents	documents	documents	documents
3.	web history	**purchases**	**purchases**	**purchases**
4.	purchases	**web history**	**photos**	**photos**
5.	photos	photos	**web history**	**calendar**
6.	calendar	calendar	calendar	**web history**

Willingness to Share Purchase Records
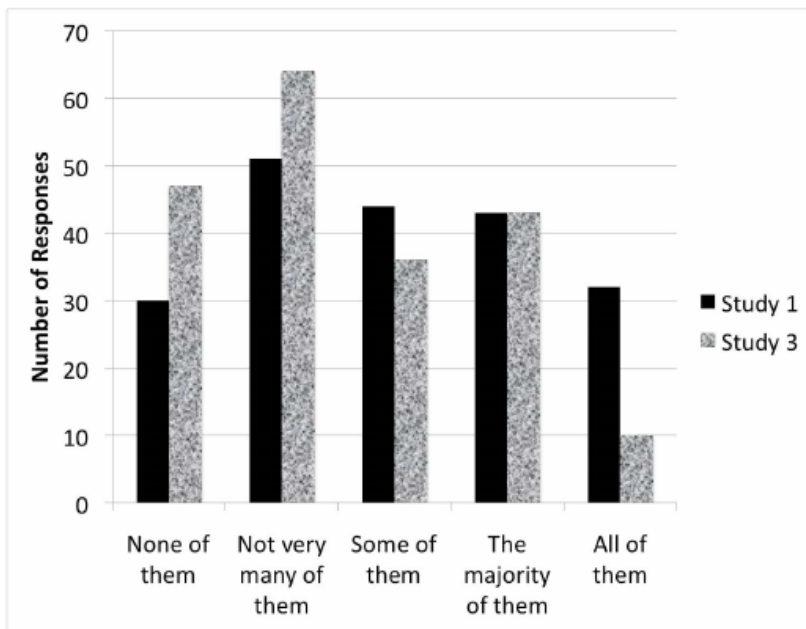
Quantifying Privacy
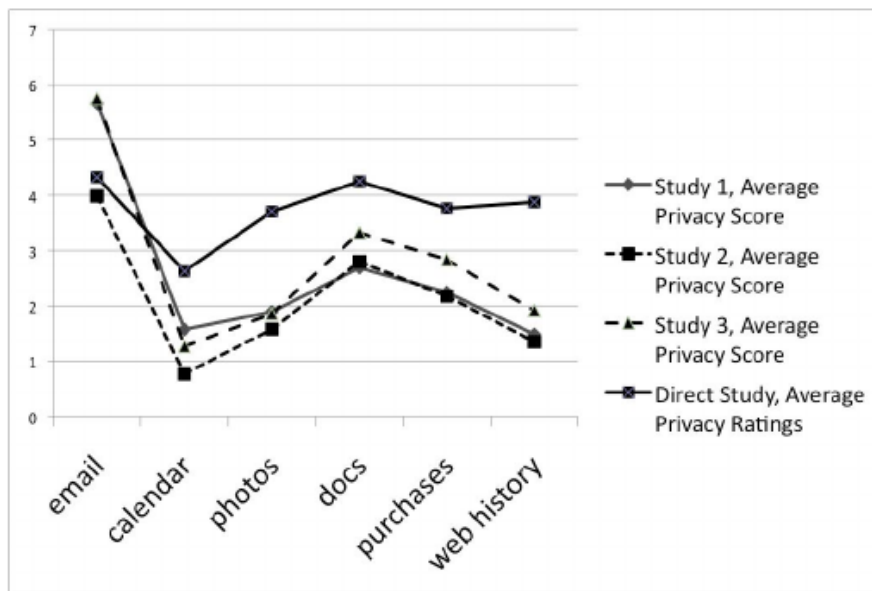
Android Permissions

Android Permissions:
User Attention, Comprehension, and Behavior

Adrienne Porter Felt*, Elizabeth Ha[†], Serge Egelman*,
Ariel Haney[†], Erika Chin*, David Wagner*
*Computer Science Department   †School of Information
University of California, Berkeley
{apf,egelman,emc,daw}@cs.berkeley.edu, {lizzy,arielhaney}@ischool.berkeley.edu

ABSTRACT

Android's permission system is intended to inform users about the risks of installing applications. When a user installs an application, he or she has the opportunity to review the application's permission requests and cancel the installation if the permissions are excessive or objectionable. We examine whether the Android permission system is effective at warning users. In particular, we evaluate whether Android users pay attention to, understand, and act on permission information during installation. We performed two usability studies: an Internet survey of 308 Android users, and a laboratory study wherein we interviewed and observed 25 Android users. Study participants displayed low attention and comprehension rates: both the Internet survey and laboratory study found that 17% of participants paid attention to permissions during installation, and only 3% of Internet survey respondents could correctly answer all three permission comprehension questions. This indicates that current Android permission warnings do not help most users make correct security decisions. However, a notable minority of users demonstrated both awareness of permission warnings and reasonable rates of comprehension. We present recommendations for improving user attention and comprehension, as well as identify open challenges.

data or sends premium SMS messages for profit. Grayware and malware have both been found in the Android Market, and the rate of new malware is increasing over time [17, 46].

Google does not review or restrict Android applications. Instead, Android uses *permissions* to alert users to privacy- or security-invasive applications. When a user initiates the process of installing an application, he or she is shown the list of permissions that the application requests. This list identifies all of the phone resources that the application will have access to if it is installed. For example, an application with the SEND_SMS permission can send text messages, but an application without that permission cannot. If the user is not comfortable with the application's permission requests, then he or she can cancel the installation. Users are not shown permissions at any time other than installation.

In this paper, we explore whether Android permissions are usable security indicators that fulfill their stated purpose: "inform the user of the capabilities [their] applications have" [5]. We base our inquiry on Wogalter's Communication-Human Information Processing (C-HIP) model, which provides a framework for structuring warning research [44]. The C-HIP model identifies a set of steps between the delivery of a warning and the user's final behavior. We connect each step with a research question:

Problem

- Android permissions don't help users make correct security decisions

Research Questions

- Attention switch and maintenance: Do users notice permissions?
- Comprehension and memory: Do users understand how permissions correspond to application risks?
- Attitudes and belief: Do users trust permissions to limit an app's abilities?
- Motivation: Do users care about their phones' privacy and security?
- Behavior: Do users ever cancel installation due to permissions?

Exercise: Summary of Results

- Attention:
  - What portion pays attention? 17%
  - What portion is unaware? 42%
- Comprehension:
  - What portion of survey participants understand permissions correctly? 3%
  - What portion of lab study participants understand permissions correctly? 24%
- Behavior: Majority claimed not installing app due to permissions at least once

Permissions at Installation Time
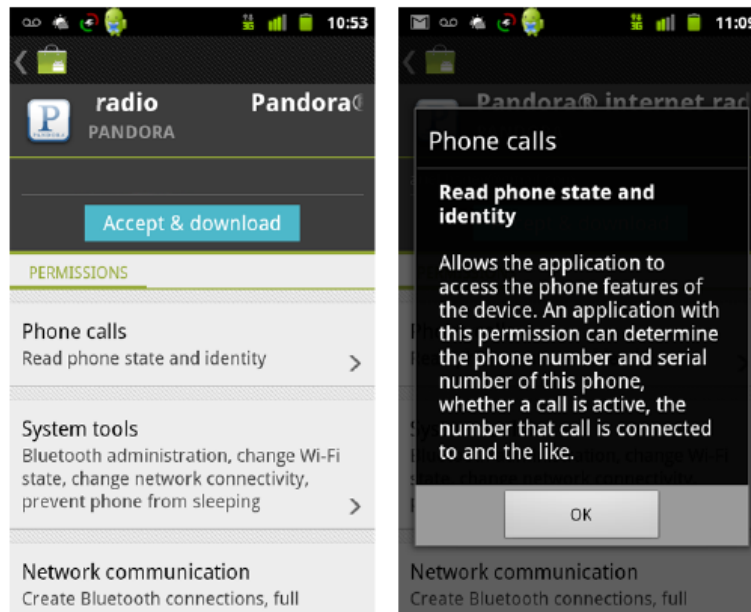
Methodology

- Internet Survey
  - Recruited Android users
  - Published ad to be displayed in apps on Android devices in US and Canada
  - Free MP3 download for every participant
  - 350 completed the survey, of which 308 had valid responses
- Lab Study
  - Recruited 25 Android users
  - Supplement the Internet survey
  - Offered $60 for an hour-long interview

Quiz Question from Internet Study
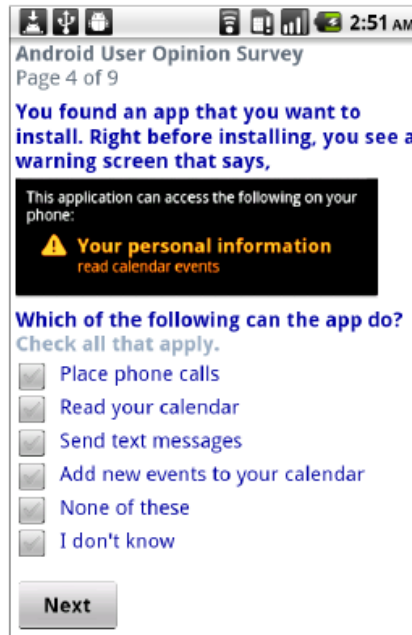
All Quiz Questions – Part I

Permission	n	Options		Responses	
INTERNET Category: Network communication Label: Full Internet access	109	✔	Send information to the application's server	45	41.3%
		✔	Load advertisements	30	27.5%
		✗	None of these	16	14.7%
		✗	Read your text messages	13	11.9%
		✗	Read your list of phone contacts	11	10.1%
			I don't know	36	33.0%
READ_PHONE_STATE Category: Phone calls Label: Read phone state and identity	85	✔	Read your phone number	41	47.7%
		✗	See who you have called	37	43.0%
		✔	Track you across applications	20	23.3%
		✗	Load advertisements	11	12.8%
		✗	None of these	10	11.6%
			I don't know	15	17.4%
CALL_PHONE Category: Services that cost you money Label: Directly call phone numbers	83	✔	Place phone calls	30	35.3%
		✗	Charge purchases to your credit card	27	31.8%
		✗	None of these	16	18.8%
		✗	See who you have made calls to	14	16.5%
		✗	Send text messages	11	12.9%
			I don't know	16	18.8%
WRITE_EXTERNAL_STORAGE Category: Storage Label: Modify/delete SD card contents	92	✔	Read other applications' files on the SD card	41	44.6%
		✔	Change other applications' files on the SD card	39	42.4%
		✗	None of these	16	17.4%
		✗	See who you have made phone calls to	15	16.3%
		✗	Send text messages	11	12.0%
			I don't know	15	16.3%
WAKE_LOCK Category: System tools Label: Prevent phone from sleeping	81	✔	Keep your phone's screen on all the time	49	60.5%
		✔	Drain your phone's battery	37	45.7%
		✗	None of these	7	8.6%
		✗	Send text messages	4	4.9%
		✗	Delete your list of contacts	4	4.9%
			I don't know	13	16.0%
CHANGE_NETWORK_STATE Category: System tools Label: Change network connectivity	66	✔	Turn your WiFi on or off	36	52.9%
		✗	Send information to the application's server	13	19.1%
		✗	Read your calendar	7	10.3%
		✗	None of these	7	10.3%
		✗	See who you have made calls to	5	7.4%
			I don't know	17	25.0%

## All Quiz Questions – Part II

READ_SMS$_2$ Category: Your messages Label: Read SMS or MMS	54	✔ Read text messages you've sent ✔ Read text messages you've received ✗ Send text messages ✗ Read your phone's unique ID ✗ None of these *I don't know*	30 25 10 6 4 11	54.5% 45.5% 18.2% 10.9% 7.3% 20.0%
READ_SMS$_1$ Category: Your messages Label: Read SMS or MMS	77	✔ Read text messages you've received ✗ Read e-mail messages you've received ✗ Read your call history ✗ None of these ✗ Access your voicemail *I don't know*	44 30 13 8 8 13	56.4% 38.5% 16.7% 10.3% 10.3% 16.7%
READ_CALENDAR Category: Your personal information Label: Read calendar events	101	✔ Read your calendar ✗ None of these ✗ Add new events to your calendar ✗ Send text messages ✗ Place phone calls *I don't know*	56 18 12 12 9 19	53.3% 17.1% 11.4% 11.4% 8.6% 18.1%
READ_CONTACTS Category: Your personal information Label: Read contact data	86	✔ Read your list of contacts ✔ Read your call history ✗ None of these ✗ Delete your list of contacts ✗ Place phone calls *I don't know*	52 19 14 9 5 14	60.5% 22.1% 16.3% 10.5% 5.8% 16.3%
CAMERA Category: Hardware controls Label: Take pictures	72	✔ Take pictures when you press the button ✔ Take pictures at any time ✔ See pictures taken by other applications ✔ Delete pictures taken by other apps ✗ None of these *I don't know*	27 27 16 13 13 17	37.0% 37.0% 21.9% 17.8% 17.8% 23.3%

Sample Task for Lab Study

- Pretend you are a little short on cash, so you want to install a coupons app. You want to be able to find coupons and sales for groceries, your favorite electronics, or clothes while you're out shopping. If you already have a coupons app, pretend you don't like it and want a new one.

Exercise: Settings Page for Lab Study
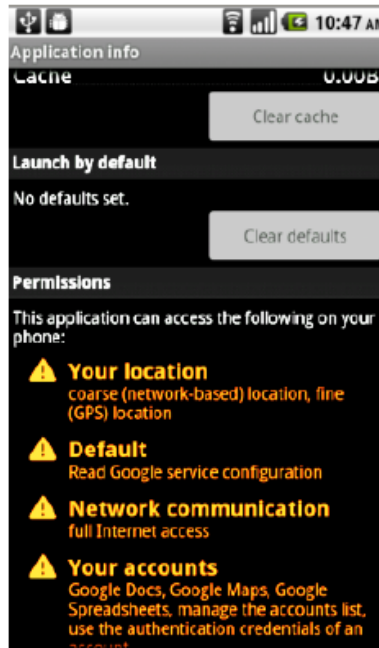
Results: Attention During Installation

Attention to Permissions	Number of users	95% CI	
Looked at the permissions	4	17%	5% to 37%
Didn't look, but aware	10	42%	22% to 63%
Is unaware of permissions	10	42%	22% to 63%

Implications

- No Control Over Permissions
- One participant said: "I used to be concerned about the location permission, but gradually lost my concern because so many of the applications that I installed requested this permission."

- App reviews: Other users might warn about undesirable or privacy-invasive apps

Participants' Grades
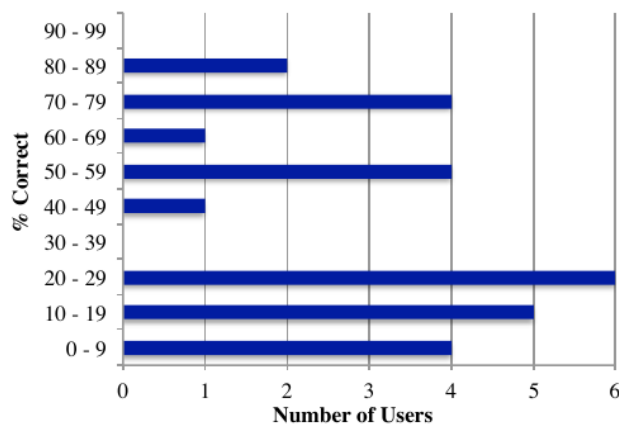
	READ_CONTACTS	WAKE_LOCK	WRITE_EXTERNAL_STORAGE	READ_PHONE_STATE	INTERNET
Correct	0%	54%	47%	0%	68%
Correct but overly broad	9%	9%	0%	0%	4%
Incomplete [and overly broad]	18%	0%	18%	45%	9%
Wrong	45%	0%	23%	20%	9%
Unable to answer	27%	36%	12%	35%	9%
Total number of participants	11	11	17	20	22

Not Installed App Because of Permissions

Self-Reported Behavior	Respondents
Yes	56.7%
Didn't like permissions	*32.6%*
Too many permissions	*16.0%*
Both	*8.1%*
No/I don't know	43.3%

Implications

- Many users cannot connect permissions to risks: Resource-focused rather than risk-focused

- Unnecessary warnings: Permissions without clear risks should not be shown

- Absent permissions: Users cannot say with certainty that a permission does not encompass a privilege

Scaling Requirements Extraction to the Crowd

Scaling Requirements Extraction to the Crowd

Experiments with Privacy Policies

Travis D. Breaux and Florian Schaub
Institute for Software Research
Carnegie Mellon University
Pittsburgh, Pennsylvania, United States
{breaux, fschaub}@cs.cmu.edu

Abstract—Natural language text sources have increasingly been used to develop new methods and tools for extracting and analyzing requirements. To validate these new approaches, researchers rely on a small number of trained experts to perform a labor-intensive manual analysis of the text. The time and resources needed to conduct manual extraction, however, has limited the size of case studies and thus the generalizability of results. To begin to address this issue, we conducted three experiments to evaluate crowdsourcing a manual requirements extraction task to a larger number of untrained workers. In these experiments, we carefully balance worker payment and overall cost, as well as worker training and data quality to study the feasibility of distributing requirements extraction to the crowd. The task consists of extracting descriptions of data collection, sharing and usage requirements from privacy policies. We present results from two pilot studies and a third experiment to justify applying a task decomposition approach to requirements extraction. Our contributions include the task decomposition workflow and three metrics for measuring worker performance. The final evaluation shows a 60% reduction in the cost of manual extraction with a 16% increase in extraction coverage.

extraction is that, when the method is derived from the dataset, called a *grounded theory* [12], the derivation process surfaces complex nuances and boundary cases that are more likely addressable using human-interpretable heuristics. Such boundary cases are often difficult to address using automated approaches. In prior work, for example, Breaux et al. discovered heuristics for inferring *implied* rights and obligations from explicitly stated requirements to increase requirements coverage [8]. However, the downside of manual methods is the challenge of scalability: achieving a two-fold increase in the number of documents processed requires considerable effort by a small number of expert analysts. Moreover, automated approaches, including machine learning, rely on large data sets to evaluate performance in cross-validation studies [3]. Overcoming this challenge of scaling manual extraction could lead to new analytics that leverage unprecedentedly large datasets.

Crowdsourcing and human computation provide a middle ground between manual extraction by a few experts and natural language processing. Crowdsourcing has emerged as a viable

---

Goal

- Extract descriptions of data collection, sharing, and usage requirements from privacy policies

- Reduce cost of extraction while preserving quality

Challenges with Crowdsourcing

- Assessment of quality of work
- Estimation of fair wage
- Mitigation strategies:
- Signaling to workers that their responses will be scrutinized
- Multi-level review: A second group of workers evaluate initial group's responses
- Competition: Multiple workers submit responses, only one is paid

Statement-level Coding

- <u>Collect:</u> Any act by a first party to access, collect, obtain, receive or acquire data from another party
- <u>Consent:</u> Any act by a party to consent to, or control the use of, their personal information
- <u>Use:</u> Any act by a first party to use data in any way for their own purpose
- <u>Retain:</u> Any act by a first part to retain data for a particular period of time or in a particular location
- <u>Transfer:</u> Any act by a first party to transfer, move, send or relocate data to another party

Phrase-level Coding

- Modality: Whether the action is a permission, obligation or prohibition
- Subject: The actor who performs the action on the datum
- Datum: The information on which the action is performed
- Purpose: The purpose for which the action is performed
- Source: The source from which information is collected
- Target: For transfer actions, the recipient to whom the information is transferred

Statement-level Coding Interface

Instructions: What action(s) does this statement describe? Check one or more boxes next to those actions *and* enter any words or phrases from the statement that indicate why you selected the action.

Statement: ${text}

☐   **Use** - an act to use personal information for a particular purpose
Use keywords: [ ]

☐   **Transfer** - an act to transfer or share personal information with another party
Transfer keywords: [ ]

☐   **Retain** - an act to retain or store personal information
Retain keywords: [ ]

☐   **Consent** - an act by a party to consent to, or control the use of, their personal information
Consent keywords: [ ]

☐   **Collect** - an act to collect personal information from another party
Collect keywords: [ ]

☐   None of the above

[Submit Query]

Phrase-level Coding Interface

In the following statement, any pronouns "We" or "Us" refer to the ${company}, and "you" refers to the ${user}.

Statement: ${text}

○ The above statement [prohibits ▾] the [transfer ▾] of...

What verb/noun in the statement indicates this action: [_____]
(e.g., transfer, share, send, etc.)

What kind of information? [_____]
Transferred by whom? [_____]
Transferred to whom? [_____]
Transferred for what reason? [_____]

○ The above statement does not describe a collection, use, retention or transfer.

[Submit Query]

Exercise: Coding I

- Statement-level: Collect, consent, use, retain, transfer
- Phrase-level: Modality, subject, datum, purpose, source, target

- "We may collect or receive information from other sources including (i) other Zynga users who choose to upload their email contacts; and (ii) third party information providers."

- "We do not actively share personal information with third party advertisers for their direct marketing purposes unless you give Us your consent."

- "Zynga stores information about site visitors and players on servers located in the United States."

Exercise: Coding II

- Statement-level: Collect, consent, use, retain, transfer
- Phrase-level: Modality, subject, datum, purpose, source, target

- "We receive and store the information you provide, including your telephone number, when you sign up to have SMS notifications sent directly to your mobile phone."

- "To properly credit user accounts and to prevent fraud, a unique identifier, in some cases your user ID number, will be shared with the offer wall provider."

- "This information will be used to supplement your profile – primarily to help you and your friends connect."

Exercise: Coding III

- Statement-level: Collect, consent, use, retain, transfer
- Phrase-level: Modality, subject, datum, purpose, source, target

- "The information collected may be used to offer you targeted ad-selection and delivery in order to personalize your user experience by ensuring that advertisements for products and services you see will appeal to you, a practice known as behavioral advertising, and to undertake web analytics (i.e. to analyze traffic and other end user activity to improve your experience)."

- "Zynga implements reasonable security measures to protect the security of your information both online and offline, and we are committed to the protection of customer information."

Worker Performance
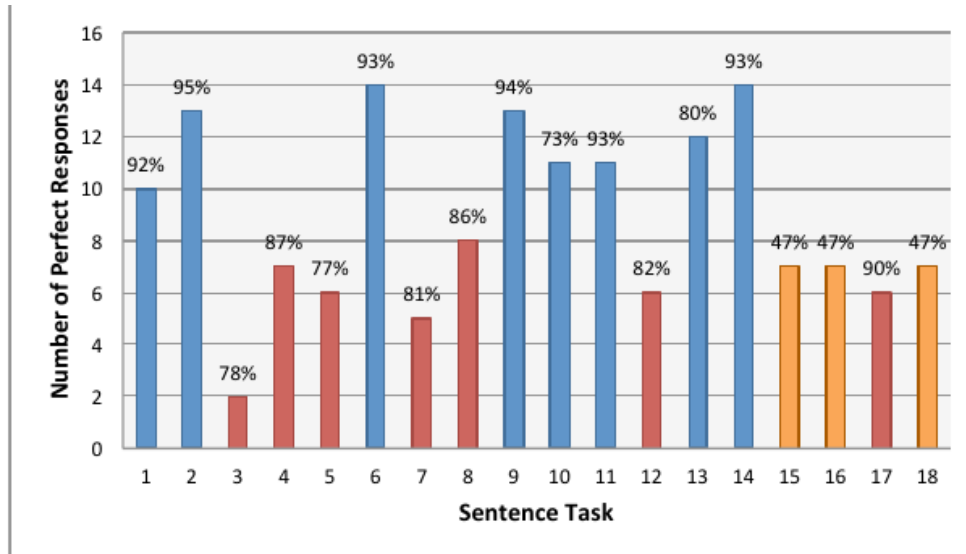
Task Decomposition

- Once a worker understands a simple task, they can more effectively perform it repeatedly compared to switching between different tasks during the same period
- Certain steps in the extraction process can be performed by automated NLP with acceptable levels of precision and recall
- Certain microtasks depend on the results from other microtasks, thus suggesting natural break points and ordering of microtasks in a task decomposition
- The financial cost of a task is directly proportional to the task complexity or cognitive demand, thus decomposition should coincide with a smaller cost per microtask, but not necessarily a smaller overall cost

Task Decomposition Workflow
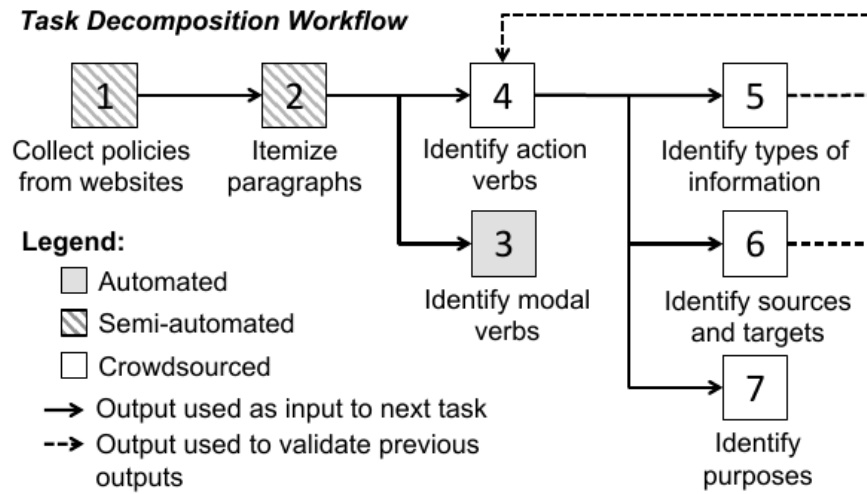
Cost Comparison

Policy	Tasks*	MTurk Fees	Total Cost	Worker Comp.
Amazon	18	$3.24	$40.64	$6.48
Rovio	18	$3.24	$40.64	$6.48
Walmart	27	$4.86	$58.46	$9.72
Waze	34	$6.12	$72.32	$12.24
Zynga	32	$5.76	$68.36	$11.52

"Brightest" Free App

- News article: https://www.ftc.gov/news-events/press-releases/2013/12/ android-flashlight-app-developer-settles-ftc-charges-it-deceived
- Links are also on the course website

Things to Look For

- Root cause: What went wrong?
- If it was not intentional, what was the original aim?
- Affected parties
- Implications and similar problems
- Mitigation (using methods we have seen): Prevention, detection, recovery

- Take 10 minutes to look at the incident on your own

- Now discuss with your neighbor