CSE711
Topics in Differential Privacy

Marco Gaboardi
Room: 338-B
gaboardi@buffalo.edu
http://www.buffalo.edu/~gaboardi

Software Applications: Services vs. Requirements

Software Applications: Services vs. Requirements

Software Applications: Services vs. Requirements

Security

Usability




Privacy

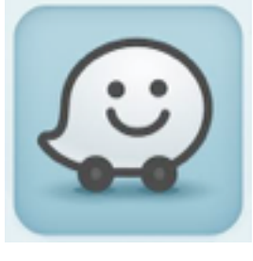
Accuracy









Efficiency

Resources

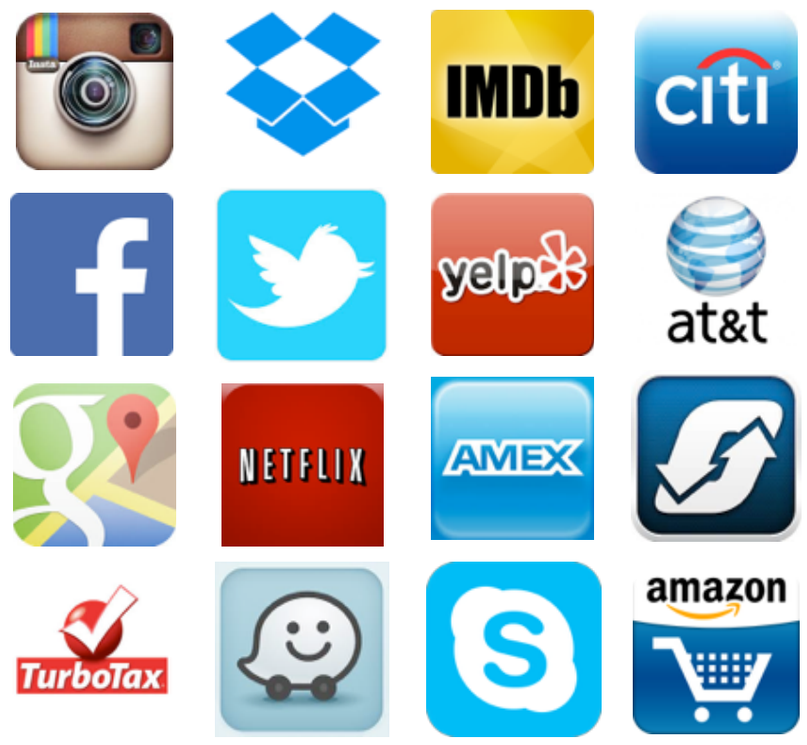
Software Applications: Services vs. Requirements

Privacy

Software Applications: Services vs. Requirements

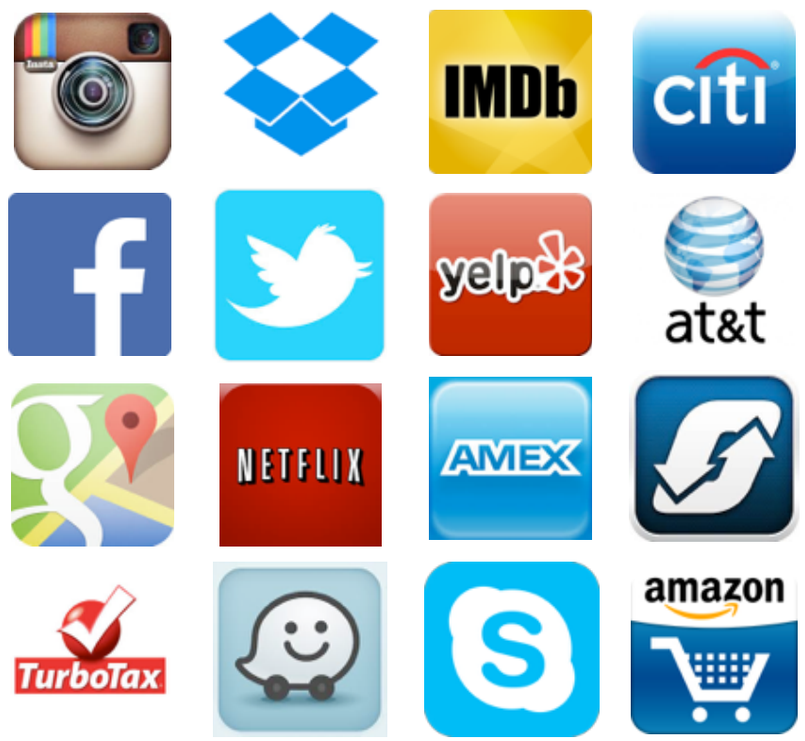
Privacy

Software Applications: Privacy Concerns



Data

Software Applications: Privacy Concerns



Anonymous Data

Software Applications: Privacy Concerns

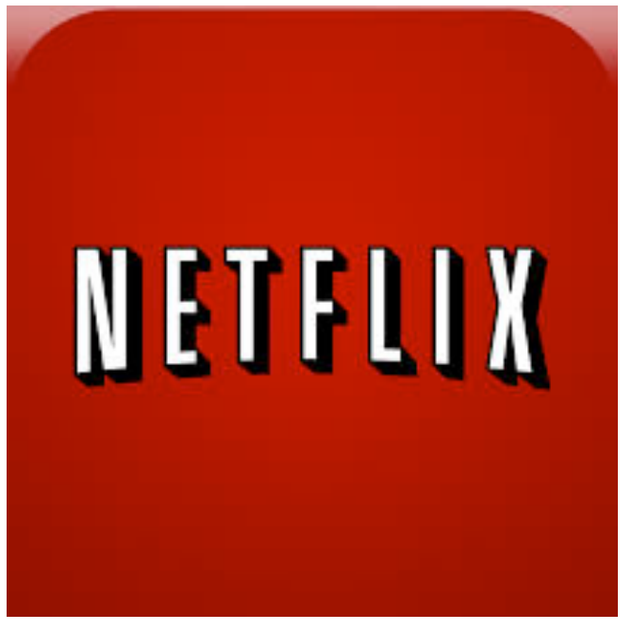
Anonymous Data

Software Applications: Privacy Concerns

Additional Data

Anonymous Data

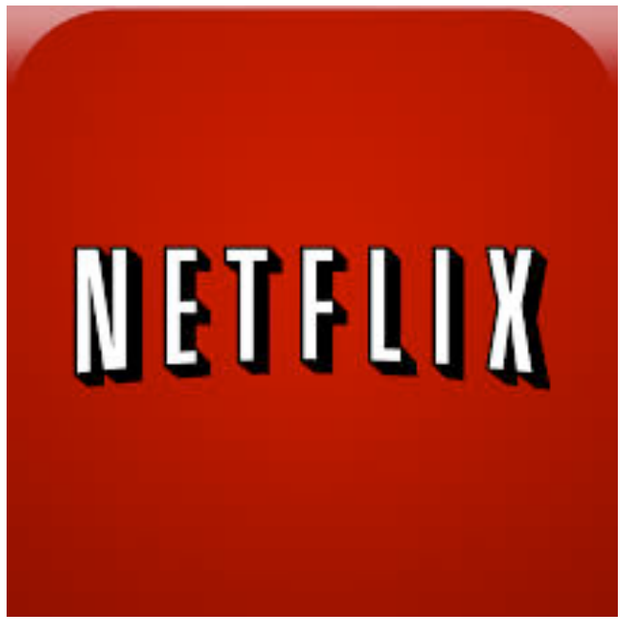
Software Applications: Privacy Concerns



Additional Data

Anonymous Data

Software Applications: Privacy Concerns



Additional Data

Anonymous Data

Challenges in Privacy: The Problem

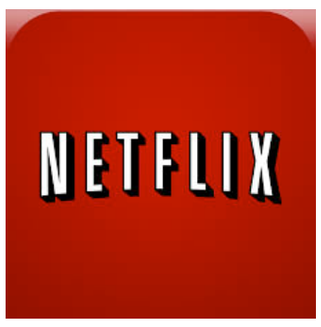
The data of an individual can have a **direct influence** on the results of a program.

Privacy vs. Utility

Privacy vs. Utility

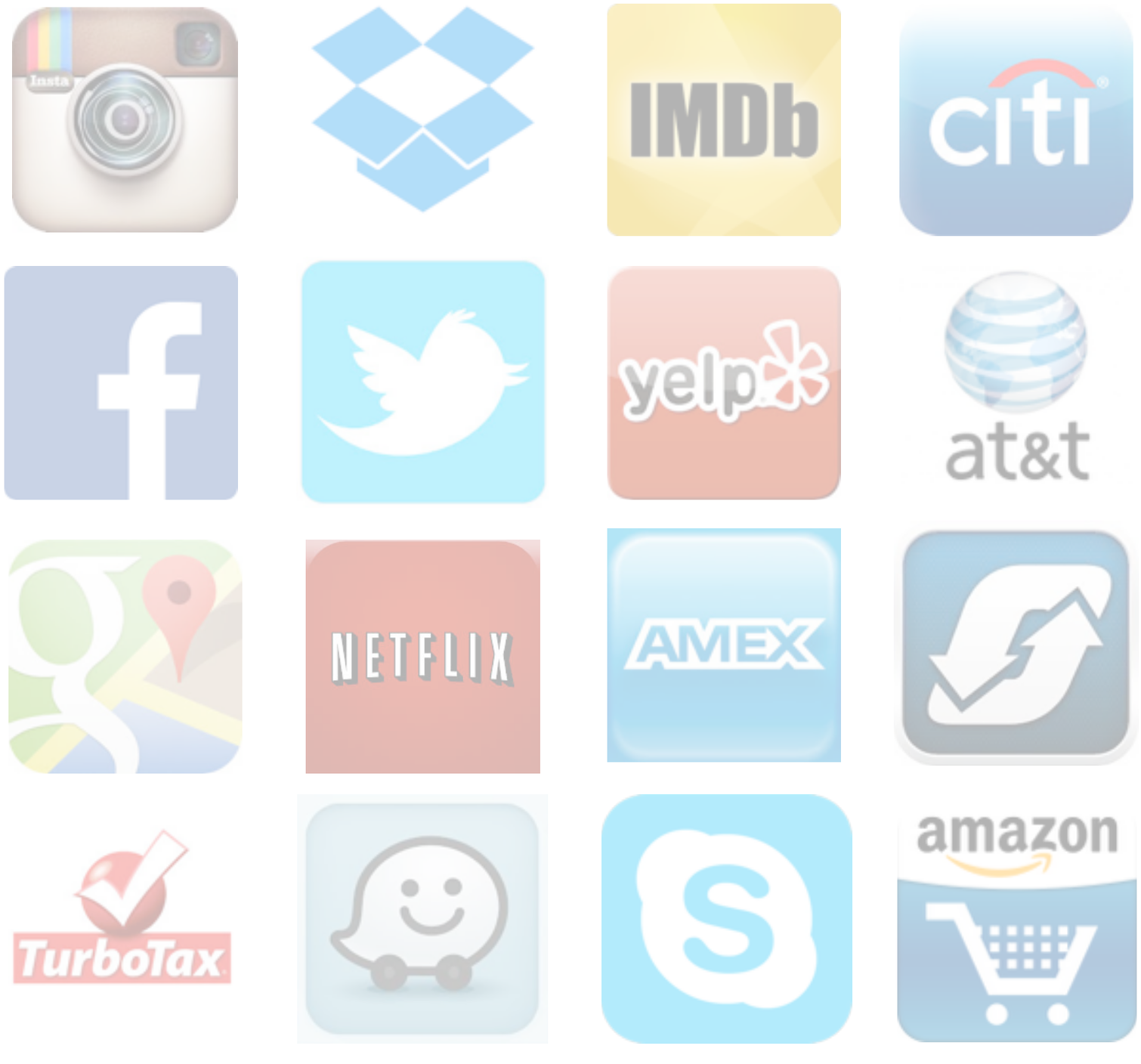









Privacy vs. Utility



Privacy **Utility**

Privacy vs. Utility

Privacy vs. Utility

Privacy vs. Utility

A Possible Solution: Differential Privacy

Syllabus for the course

Location: Davis 113A
Time: Thursday 10:30 - 12:00
Credits: 3 (Possible also to take it for 1 or 2)
Office Hours: Thursday 12:00 - 1:00 or by appointment
Discussion forums: NB and Piazza (by invitation)

Course load:
- presenting a research paper,
- commenting on the papers presented every week, beforehand on NB and during class,
- working on a project and presenting the results or alternatively presenting another paper

Grading

30% - paper presentation
40% - engagement and participation in class and on NB and Piazza
30% - project or other article presentation

Schedule

Date	Topic	Presenter
1/28	Introduction to Differential Privacy - basic definitions and mechanisms Optional reading: Chapter 1 and 2 of The Algorithmic Foundations of Differential Privacy, Dwork and Roth, 2014.	Marco Gaboardi Notes
2/04		
2/11		
2/18		
2/25		
3/3		
3/10		
3/17	No class - Spring Break	
3/24		
3/31	No class	
4/7		
4/14		
4/21		
4/28		
5/5	Project Presentation	
5/12	Project Presentation	

Articles

A - Algorithms and theory

1 - Cynthia Dwork, Guy N. Rothblum, Salil P. Vadhan: Boosting and Differential Privacy. FOCS 2010: 51-60

2 - Kamalika Chaudhuri, Daniel Hsu, Shuang Song: The Large Margin Mechanism for Differentially Private Maximization. NIPS 2014: 1287-1295

3 - Justin Hsu, Zhiyi Huang, Aaron Roth, Zhiwei Steven Wu: Jointly Private Convex Programming. SODA 2016: 580-599

4 - Cynthia Dwork, Moni Naor, Toniann Pitassi, Guy N. Rothblum: Differential privacy under continual observation. STOC 2010: 715-724

5 - Mark Bun, Jonathan Ullman, Salil P. Vadhan: Fingerprinting codes and the price of approximate differential privacy. STOC 2014: 1-10

Articles

B - Machine learning

1 - Jaewoo Lee, Yue Wang, Daniel Kifer: Maximum Likelihood Postprocessing for Differential Privacy under Consistency Constraints. KDD 2015: 635-644

2 - Moritz Hardt, Katrina Ligett, Frank McSherry: A Simple and Practical Algorithm for Differentially Private Data Release. NIPS 2012: 2348-2356

3 - Shiva Prasad Kasiviswanathan, Homin K. Lee, Kobbi Nissim, Sofya Raskhodnikova, Adam Smith: What Can We Learn Privately? FOCS 2008: 531-540

4 - Zuhe Zhang, Benjamin Rubinstein and Christos Dimitrakakis On the Differential Privacy of Bayesian Inference AAAI 2016.

5 - Christos Dimitrakakis, Blaine Nelson, Aikaterini Mitrokotsa, Bejnamin Rubinstein. Robust and private Bayesian inference Algorithmic Learning Theory (ALT-2014).

Articles

C - Privacy, Security and Cryptography

1 - Yevgeniy Dodis, Adriana López-Alt, Ilya Mironov, Salil P. Vadhan: Differential Privacy with Imperfect Randomness. CRYPTO 2012: 497-516

2 - Cynthia Dwork, Moni Naor, Salil P. Vadhan: The Privacy of the Analyst and the Power of the State. FOCS 2012: 400-409

3 - Daniel Kifer and Ashwin Machanavajjhala. A Rigorous and Customizable Framework for Privacy. PODS 2012.

4 - Daniel Kifer and Ashwin Machanavajjhala. No Free Lunch in Data Privacy. SIGMOD 2011

5 - Florian Tramèr, Zhicong Huang, Jean-Pierre Hubaux, Erman Ayday: Differential Privacy with Bounded Priors: Reconciling Utility and Privacy in Genome-Wide Association Studies. ACM CCS 2015: 1286-1297

Articles

D - Programming Languages

1- Frank McSherry: Privacy integrated queries: an extensible platform for privacy-preserving data analysis. SIGMOD Conference 2009: 19-30

2 - Gilles Barthe, Boris Köpf, Federico Olmedo, Santiago Zanella Béguelin: Probabilistic relational reasoning for differential privacy. POPL 2012: 97-110

3 - Jason Reed, Benjamin C. Pierce: Distance makes the types grow stronger: a calculus for differential privacy. ICFP 2010: 157-168

4 - Hamid Ebadi, David Sands, Gerardo Schneider: Differential Privacy: Now it's Getting Personal. POPL 2015: 69-81

5 - Lili Xu, Konstantinos Chatzikokolakis, Huimin Lin: Metrics for Differential Privacy in Concurrent Systems. FORTE 2014: 199-215

Articles

E - Systems and Databases

1 - Úlfar Erlingsson, Vasyl Pihur, Aleksandra Korolova: RAPPOR: Randomized Aggregatable Privacy-Preserving Ordinal Response. ACM Conference on Computer and Communications Security 2014: 1054-1067

2 - Georgios Kellaris, Stavros Papadopoulos, Xiaokui Xiao, Dimitris Papadias: Differentially Private Event Sequences over Infinite Streams. PVLDB 7(12): 1155-1166 (2014)

3 - Prashanth Mohan, Abhradeep Thakurta, Elaine Shi, Dawn Song, David E. Culler: GUPT: privacy preserving data analysis made easy. SIGMOD Conference 2012: 349-360

4 - Fabienne Eigner, Matteo Maffei, Ivan Pryvalov, Francesca Pampaloni, Aniket Kate: Differentially private data aggregation with optimal utility. ACSAC 2014: 316-325

5 - Arjun Narayan, Ariel Feldman, Antonis Papadimitriou, Andreas Haeberlen: Verifiable differential privacy. EuroSys 2015: 28:1-28:14

Articles

F - Applications to other areas

1 - Konstantinos Chatzikokolakis, Catuscia Palamidessi, Marco Stronati: Geo-indistinguishability: A Principled Approach to Location Privacy. ICDCIT 2015: 49-72

2 - Cynthia Dwork, Moritz Hardt, Toniann Pitassi, Omer Reingold, Richard S. Zemel: Fairness through awareness. ITCS 2012: 214-226

3 - Cynthia Dwork, Vitaly Feldman, Moritz Hardt, Toniann Pitassi, Omer Reingold, Aaron Roth: Generalization in Adaptive Data Analysis and Holdout Reuse. CoRR abs/1506.02629 (2015)

4 - Cynthia Dwork, Adam D. Smith, Thomas Steinke, Jonathan Ullman, Salil P. Vadhan: Robust Traceability from Trace Amounts. FOCS 2015: 650-669

5 - Mário S. Alvim, Miguel E. Andrés, Konstantinos Chatzikokolakis, Catuscia Palamidessi: On the Relation between Differential Privacy and Quantitative Information Flow. ICALP (2) 2011: 60-76.

6 - Frank McSherry, Kunal Talwar: Mechanism Design via Differential Privacy. FOCS 2007.

Reference Book

Cynthia Dwork and Aaron Roth,
"The Algorithmic Foundations of Differential Privacy,"
Foundations and Trends in Theoretical Computer Science, Vol 9,
Nos 3–4, pp. 211–407, 2014.
PDF file available on Aaron Roth's webpage.

Questions?