

What Cryptography and TCS can do for Law

SHAFI GOLDWASSER

Thanks to K. Bamberger, R. Canetti, A. Cohen, F. Partnoy,
Y. Shavit, M. Varia, P. Vasudevan, and D. Weitzner

My Journey into “Law For Algorithm”[Y]



- Law for Algorithms Fall 2018
 - Boston University, Harvard, Columbia, Berkeley
(Canetti, Caruso, Dugan, Dwork, Minow, Williams, Goldwasser)
- Law for Algorithms Fall 2019
 - Boston University and Berkeley
(Canetti, Dugan, Goldwasser, Partnoy)
- Danny Weitzner: Cohen, Frankle, Park, Shavit Fall 2017

Lessons Learned

Language Barrier

Knowledge Barrier

Clear: Need Interdisciplinary effort between law and computer science, to bridge the gap between legal standards and algorithms which stand to govern of our life

Time is Ripe

Law for Governing Algorithms

Algorithms for Implementing Law

Outline

- **The Power of Formal Definitions:**
Mathematically (crypto style) define
“The Right to be Forgotten: Discover How to be Compliant”
[GGV2019, in submission]
- **Potential** of using cryptographic protocols such as ZK and MPC for new and better legal procedures
- **Case in point:** Encryption Debate of Surveillance vs. Government Accountability
“Practical Applicability of Secret Processes”
[FPSGW, USENIX2018]

AVAILABILITY OF DATA ABOUT INDIVIDUALS HAS ENORMOUS POTENTIAL TO BETTER OUR LIVES

- **Health:** disease control by trend prediction
- **Finance:** predictions for financial markets
- **Economic Growth:** intelligent consumer targeting
- **Infrastructure:** Traffic patterns and energy usage
- **Vision:** Facial and Image recognition
- **NLP:** Speech recognition, Machine Translation
- **Security:** Threat Prediction models, spam
- **Policing:** decide which neighborhood to police
- **Bail :** decide who is a flight risk
- **Credit Rating:** decide who gets a loan

Sudden Shift of Power



Privacy Regulations: Discussed, Codified, Made into Law



CCPA

- Requires consent from the individual
- Wide definition of personal information including browser history, purchase behaviour, site/app interactions
- Allows for opt-out of collection/use
- Fines potentially in the millions of dollars
- Private right of action, class suits



GDPR

- Has a legitimate interest component
- Defines PII and sensitive information
- Default to opt-in for collection/use
- Fines potentially in the millions of dollars
- Public complaints to an enforcement body to address

10⁶ Q: AM I COMPLIANT?

Why “The Right to be Forgotten” ?

EU court backs 'right to be forgotten': Google must amend results on request

Individuals have right to control their data and can ask search engines to remove results, says European court

If You Want Life Insurance, Think Twice Before Getting A Genetic Test

FASTCOMPANY

The test case privacy ruling by the European Union's court of

justice against Google Spain was brought by a Spanish man,
As genetic testing explodes, health insurers are banned from dipping into gene base

Center for American Progress

Search

ISSUES EXPERTS EVENTS PRESS ABOUT DONATE

TRENDING: TRUMP'S CONSTITUTIONAL CRISIS DACA CHINA HEALTH CA

CRIMINAL JUSTICE

Mario Costeja González, after he failed to secure the deletion
of an auction notice of his repossessed home dating from 1998
on the website of a mass circulation newspaper in Catalonia.

But How ?

Six States Leading the Charge on Second-Chance Policies

To Determine Compliance Need to Formally Define “Data Deletion”

“The Right to be Forgotten: Discover How to be Compliant”

Joint work with Garg and Vasudevan
[in submission]



[NBWBGGOVS17] “Bridging the Gap between Computer Science and Legal Approaches to Privacy”, 2017

[CN19] “Towards Formalizing the GDPR Notion of Singling Out”, 2019

Data Privacy Laws

Data Privacy Techniques

HIPAA,
GDPR,

Do techniques satisfy
Laws?

Right to be forgotten
(or to be forgotten)

“right to withdraw consent at any time.. Right to object if their personal data is processed...by processors”...

Computation
Obfuscation
Pseudonymization,
K-anonymity,
Differential Privacy

...

Legal Analysis

Mathematical
Modeling &
Analysis

1. **Extract** relevant
text

2. **Define** mathematically

4. **Solicit** legal
opinions

3. **Analyze** taking into
account other notions and
attacks +

Design Mechanisms to
Provably Achieve Definition

Iterative Process

GDPR → Personal Data → erasure

GDPR lists conditions when an entity may lawfully process personal data. “the data subject has given consent to the processing of his or her personal data for one or more specific purposes”.

[Article 6]

“The data subject shall have the right to **withdraw** his or her **consent** at any time”

[Article 7]

“The data subject shall have the right to obtain from **the controller** the **erasure** of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay ... [under a number of conditions]”

[Article 17]

Defining Data Deletion: more than meets the eye

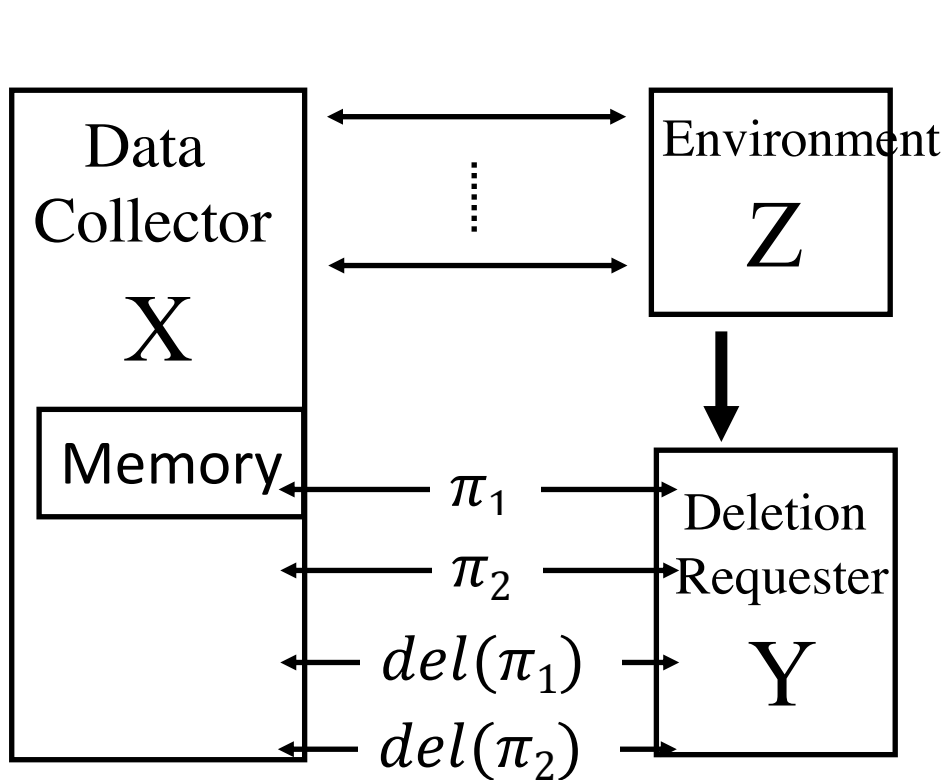
- Data Leaves May Traces
- Main Question: how does an **honest data collector** know it is doing its erasing as the law requires?

Objectives of a First Definition

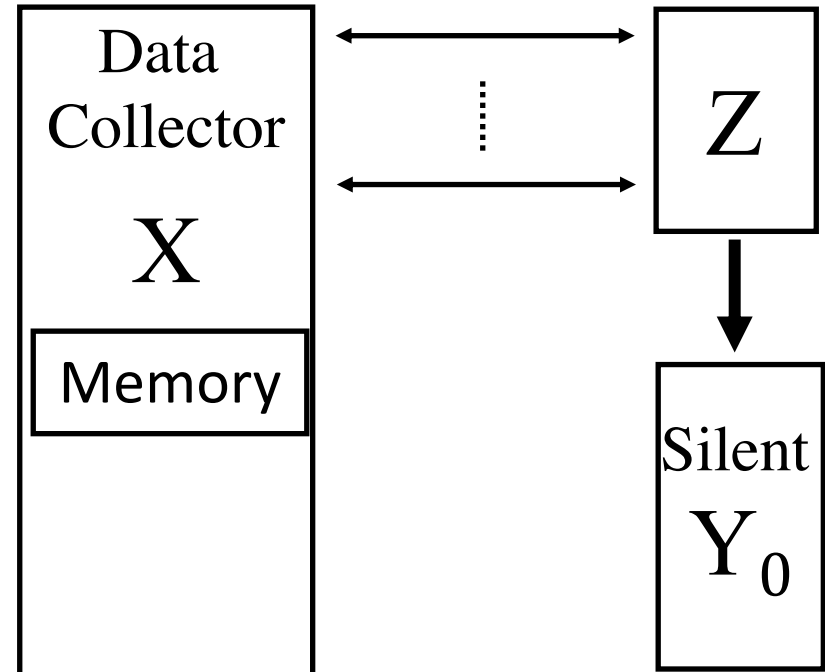
- **Generality** making as few assumptions as possible about how the system used the data
- **Simplicity**
- **Provides Protection As intended**

Defining Data Deletion: Real-Ideal definition

Real World:



Ideal World:

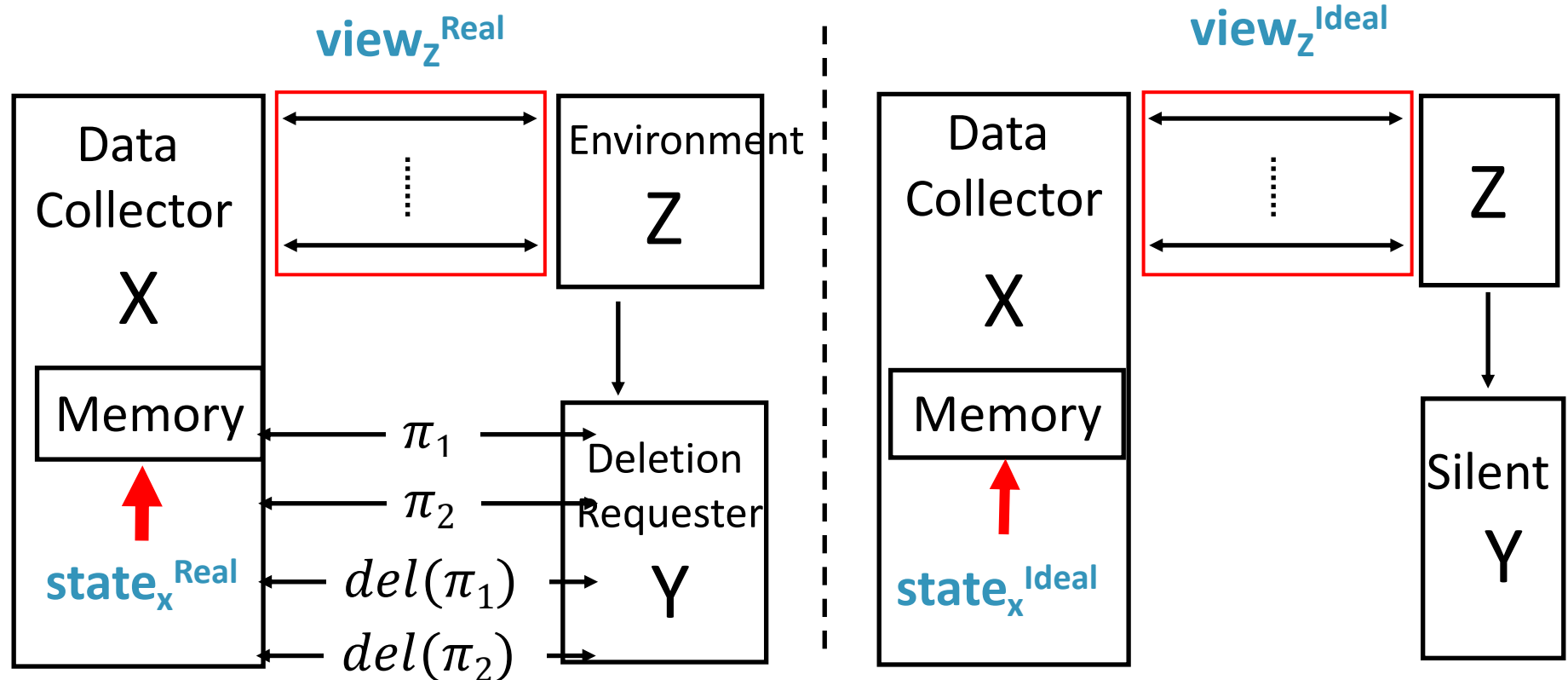


(no communication)

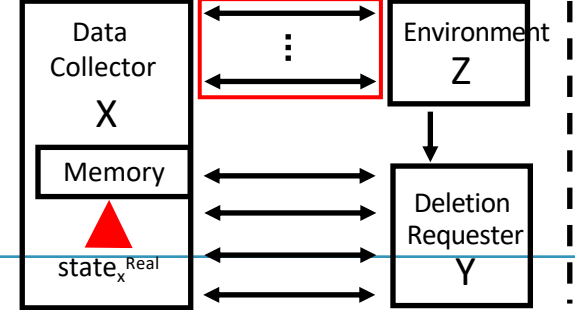
Deletion Compliance

Real World:

Ideal World:



X is **deletion-compliant** if for all Z and Y,
 $(state_x^{Real}, view_z^{Real}) \approx (state_x^{Ideal}, view_z^{Ideal})$

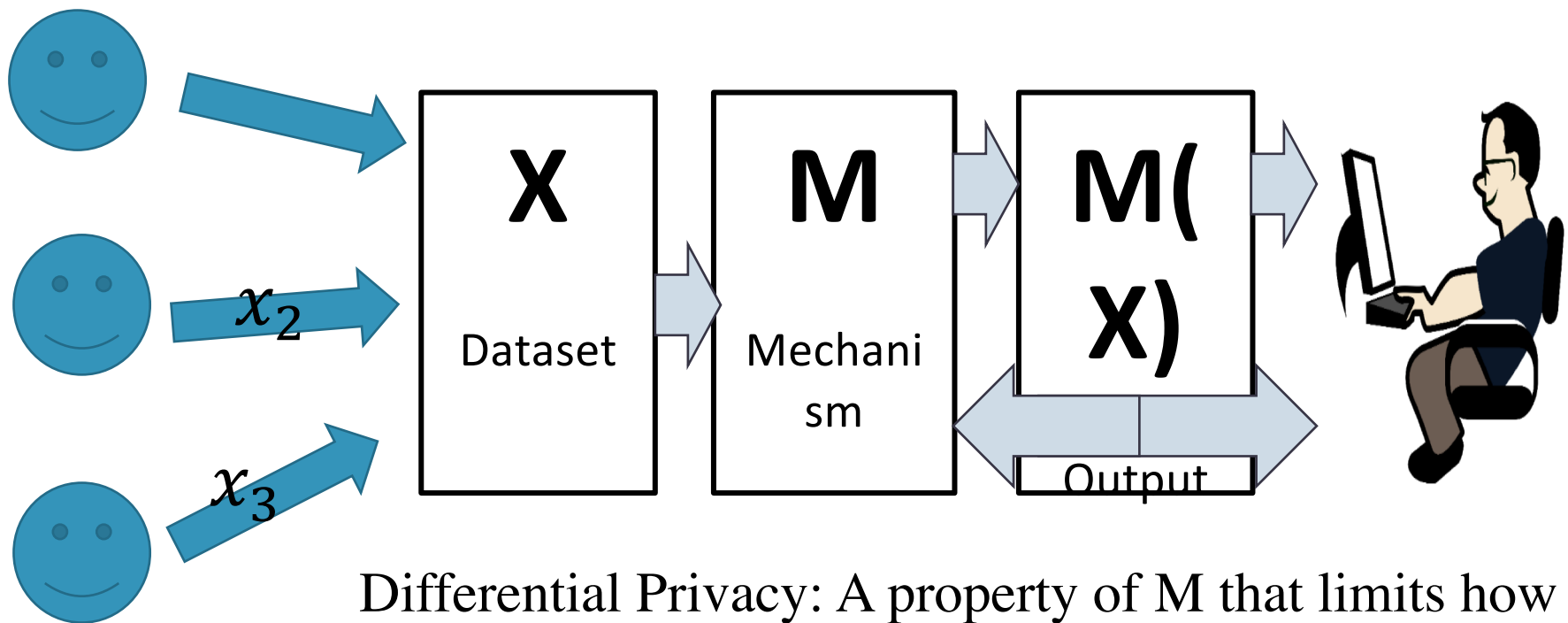


Ex: Data Storage

- A data structure has
 - A “*legitimate*” interface: the set of operations allowed to be performed on it [Insert replace Delete]
 - A memory representation
- **Techniques:** History Oblivious data structures: randomized operations [Micciancio97, NaorTeague98]
- **Definition:** A data structure is **history oblivious** if any two sequences of operations S_1 and S_2 that yield the same content induce the same probability distribution on memory representation
- **Theorem;** Using history oblivious data structure + authentication can achieve deletion-compliance

Example : DP data release

- Sometimes, if output depends little “enough” on single inputs, don’t need to do anything else to delete.



Differential Privacy: A property of M that limits how much the output $M(x)$ depends on any single x

Example: ML Deletion

- Sometimes “history-independence” in other settings can be used to do deletion.
- Machine Learning Training Input Protection
- [SRS17] Congzheng Song, Thomas Ristenpart, and Vitaly Shmatikov. Machine learning models that remember too much. CCS 2017
- [VBE18] Algorithms that remember: Model inversion attacks and data protection law.

Remarks and Open Directions

- Our definition is very strong.

Can a weaker definition provide a reasonable compromise at some settings (conditional compliance)?

- Which definition would be useful where?
- Composition of interacting compliant data collector subsystems?
- Better understanding of **when** it is required of a data collector to honor a given deletion request.

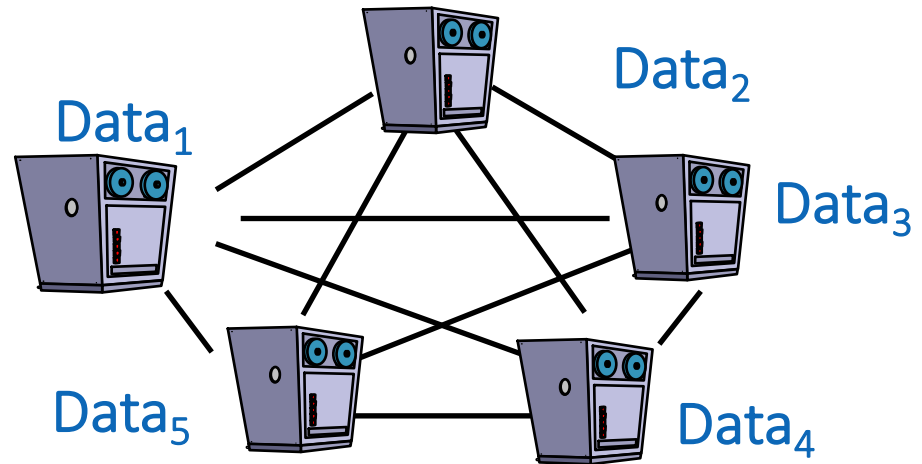
Outline

- ✓ **The Power of Formal Definitions:**
Mathematically (crypto style) define
“The right to be Forgotten: Discover How to be Compliant”
[GGV2019, in submission]
- **Potential** of using cryptographic Notions and Protocols for new and better legal procedures
 1. **Secure Multi Party Computation:** enable detecting injustice (e.g bias) without violating privacy
 2. **Zero Knowledge Proofs:** enables accountability and compliance without learning the facts

Secure Multi-Party Computation

Compute safely on shared data

[Y86, GMW86,
BGW87...]



Theorem: Distrustful parties can run arbitrary programs on the collective data **without ever revealing individual** data to each other [Under a variety of conditions]
Revealing the result, and nothing but the result

conditions : secret communication and/or good majority

Congressional definition



(12) SECURE MULTI-PARTY COMPUTATION.—The term “secure multi-party computation” means a computerized system that enables different participating entities in possession of private sets of data to link and aggregate their data sets for the exclusive purpose of performing a finite number of pre-approved computations without transferring or otherwise revealing any private data to each other or anyone else.

Dana Farber Hospital



MGH



MPC can positively benefit Impact Policy and Law



Protocol



Ex: Fusing Data Sets Data Sets for medical discovery and treatment

Detect and Address Discrimination without Finding Out Protected Attributes

Mulligan & Bamberger19: Enforcing “Privacy by Design” to reduce or eliminate the collection of data containing race and protected attributes, may make it impossible to determine “unequal treatment” via latent, redundant encoding of protected attributes and even normalize mass biases.

Proposal: Instead run MPC on collective data to gather information about “bias” and “fairness”, without learning protected attributes of individuals. Has the **potentially** relieve tension between **Disparate Treatment** vs. **Disparate Outcome**

Legal Q: Can you argue that an MPC based protocol in which you know there is a decision based on protected attribute but does not reveal protected attribute of individual does not constitute disparate treatment

The Carpenter Case

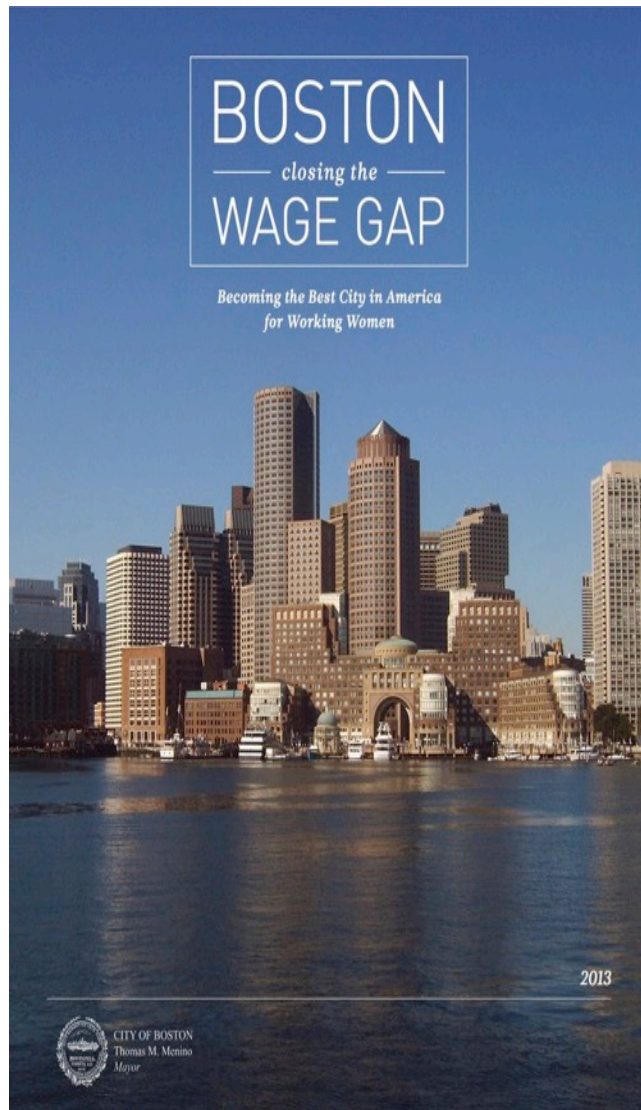


Following tip, law enforcement compelled two cell phone companies to provide continuous location information (12,898 location points) of cell-phones of several suspects (Carpenter included), over a period of 127 days.

- Carpenter moved to suppress evidence due to 4th Amendment violation. Motion denied by federal court.
- In a remarkable decision, the supreme court decided that the acquisition of data by law enforcement was in violation of Carpenter's 4th amendment rights.
- **Proposal:** Use MPC to determine if there is sufficient cause to allow surveillance

Its Been Done!

Evaluate Wage (dis)parity by BU researchers



100% TALENT

The Boston Women's Compact



STATE STREET



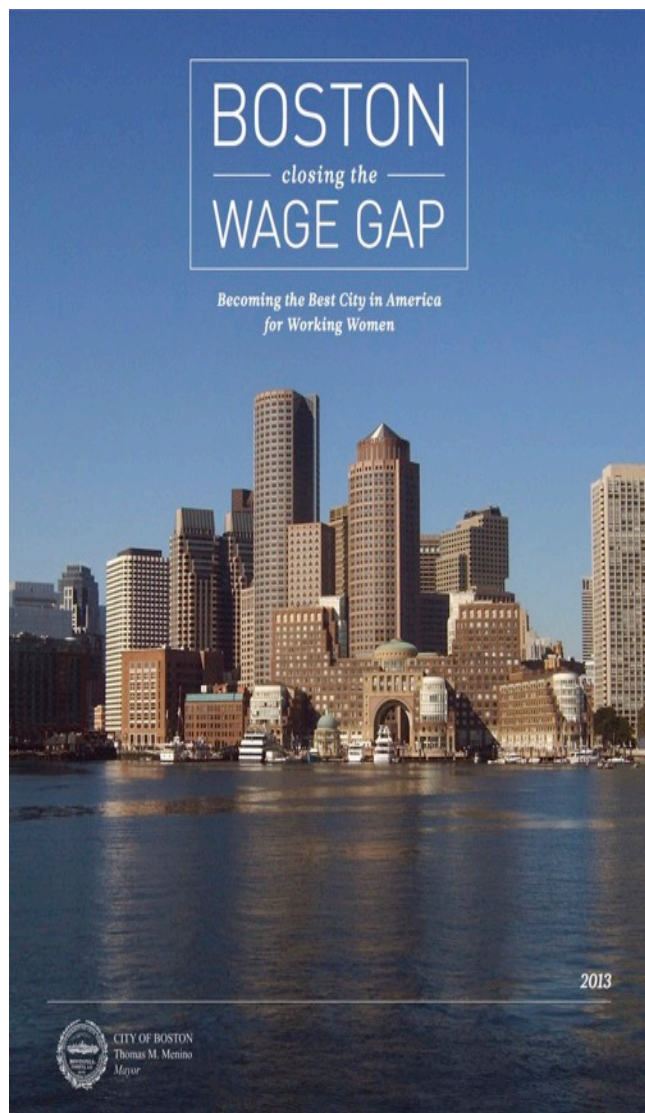
Raytheon



nationalgrid



Goal: Benchmark Wage (dis)parity



100% TALENT

Goal: Evaluating Success

Employers agree to contribute data to a report *compiled by a third party* on the Compact's success to date. *Employer-level data could not be identified* in the report.

Machine Learning Governance

Ensure Algorithms for Bail, Credit, Policing are consistent with specs

verifying data analysis

Text from CA compass case

Blackbox vversus checking

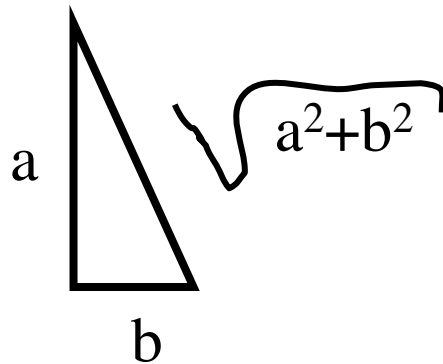
Potential legal aspects of “secure computation”

Scenarios:

1. Private entities engage in a secure computation on the union of their proprietary data.
2. Same, but data is protected by regulation (HIPAA, FERPA, FCRA, SRTLBYGA...)
3. Government performing SC on collected [potentially personal] data
4. Same, but SC performed by private entities
5. Adjudication (administrative or in courts) regarding private information
6. Same, but with non-US entities (state and private)

Each scenario has a different set of concerns... let's try to list.

Mathematical Proofs



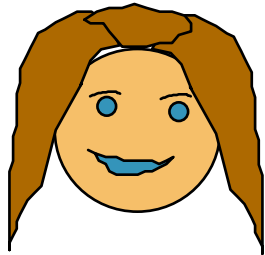
Given: $\overline{AC} \perp \overline{BD}$ $\overline{BC} \cong \overline{EC}$ $\overline{AB}$ is not $\cong$ to $\overline{ED}$ Prove: $\angle B$ is not $\cong$ to $\angle CED$	
Statements	Reasons
A 1. Assume: $\angle B \cong \angle CED$ 2. $\overline{AC} \perp \overline{BD}$ 3. $\angle BCA$ and $\angle DCE$ are right $\angle$s A 4. $\angle BCA \cong \angle ECD$ S 5. $\overline{BC} \cong \overline{EC}$ 6. $\triangle BCA \cong \triangle ECD$ 7. $\overline{AB} \cong \overline{ED}$ 8. $\overline{AB}$ is not $\cong$ to $\overline{ED}$	1. Assumption 2. Given 3. Defn. of $\perp$ segs 4. RAT 5. Given 6. ASA (1, 5, 4) 7. CPCTC 8. Given
But statement 7 contradicts statement 8. Consequently, the assumption must be false. $\therefore \angle B$ is not $\cong$ to $\angle CED$	

Efficiently Verifiable Proofs

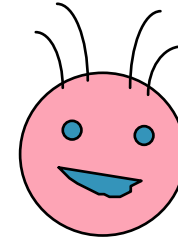
Prover Algorithm

Verifier Algorithm

Claim



proof



Checks proof

Accept or
Reject

Harder Job

Easier Job

(may know something
which the verifier does not)

Completeness: if claim true, there exist a prover algorithm that will make the Verifier algorithm Accept

Soundness: if claim false, no prover algorithm can make the Verifier algorithm accept

Revisit the Factoring Problem

Factoring: find the prime factors of a number

Number

Prime factors?

35 =

Trivial: $5 * 7$

221 =

Quick: $13 * 17$

562137 =

Long time for some humans

“1000 digit
number” =

1000 years fastest computer



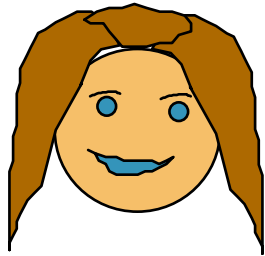
Carl Friedrich Gauss
1777-1855

“The *dignity of science* itself seems to require that every possible means be explored for the solution of a problem so elegant.”

Unless the computer is a quantum-computer

Claim: $N=pq$ where p and q are primes

Prover Algorithm



Find p and q

p and q



Verifier Algorithm



Accept or reject

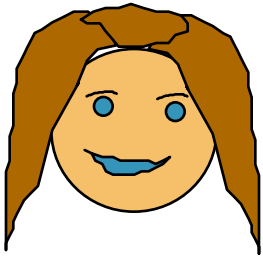
Checks that p and q
are primes and $N=pq$
Efficient

Completeness If $N=pq$, there exist a prover who can make
Verifier accept

Soundness If $N \neq pq$, such prover doesn't exist

Claim: N is a product of 2 primes

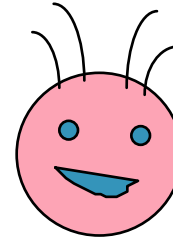
Prover Algorithm



p, q



Verifier Algorithm



Checks proof

Accept if

Solves equation

After interaction, Verifier knows:

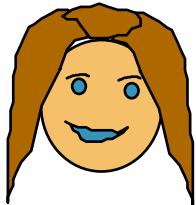
- 1) N is product of 2 primes
- 2) p and q

Is there any
other way?

Zero Knowledge Proofs

[GMicaliRackoff85, GoldrMicaliWig87]

Proofs that reveal nothing
but their validity



Main Idea:
Prove that
I could prove it
If I felt like it
and therefore a
proof exists

The Knowledge Complexity of Interactive Proof-Systems

(Extended Abstract)

Shafi Goldwasser MIT
Silvio Micali MIT
Charles Rackoff University of Toronto

1. Introduction

In the first part of the paper we introduce a new decommitting procedure, that is a new efficient method of communicating a proof. Any such method implies, directly or indirectly, a definition of proof. Our "proofs" are probabilistic in nature. On input an n -bit long statement, we may erroneously be convinced of its correctness with very small probability, say, $\frac{1}{2^n}$, and negatively be convinced of its correctness with very high probability, say, $1 - \frac{1}{2^n}$. Our proofs are interactive. To efficiently verify the correctness of a statement, the "recipient" of the proof must actively ask questions and receive answers from the "prover".

In the second part of the paper, we address the following question:

How much knowledge should be communicated for proving a theorem T ?

Certainly enough to see that T is true, but usually much more. For instance, to prove that a graph is Hamiltonian is sufficient to exhibit an Hamiltonian tour. This appears, however, to require much additional knowledge than the single bit "Hamiltonian/non-Hamiltonian".

We give a computational complexity measure of knowledge and measure the amount of additional knowledge contained in proofs.

Permission to copy without fee all or part of this material is granted provided that the copies are not made for advertising or promotional purposes, the ACM copyright notice and the title of the publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

© 1985 ACM 0-89791-151-2/85/005-0291 \$08.75

We propose to classify languages according to the amount of additional knowledge that must be released for proving membership in them.

Of particular interest is the case where this additional knowledge is essentially 0 and we show that it is possible to interactively prove that a number is quadratic non-residue mod n releasing 0 additional knowledge. This is surprising as no efficient algorithm for deciding quadratic residuosity mod n is known when n 's factorization is not given. Moreover, all known NP-proofs for this problem require the prime factorization of n . This indicates that adding interaction to the proving process, may decrease the amount of knowledge that must be communicated in order to prove a theorem.

2. Interactive Proof Systems

Much effort has been previously devoted to make precise the notion of a decommitting procedure. NP constitutes a very successful formalization of this notion. Loosely speaking, a theorem is provable in NP if its proof is easy to verify once it has been found. Let us recall Cook's [C] (and independently Levin's [L]) influential definition of NP in this light.

The NP proof-system consists of two communicating Turing machines A and B ; respectively, the prover and the verifier. The prover is exponential-time, the verifier is polynomial-time. Both A and B are deterministic, read a common input and interact in a very elementary way. On this model was suggested in part by IBM Young Faculty Development Award Award September 1983, 1984 Young Faculty Development Award April September 1986, and NSF grant DCR 8610177.

Proofs that Yield Nothing But Their Validity or All Languages in NP Have Zero-Knowledge Proof Systems

OSSED GOLDBERGH

Toronto, Ontario, Canada

SILVIO MICALI

Massachusetts Institute of Technology, Cambridge, Massachusetts

AND

AVI WIGDERSON

Hebrew University, Jerusalem, Israel

Abstract. In this paper the possibility and utility of zero-knowledge proofs, a notion introduced by Goldwasser, Micali, and Rackoff in [GM85], is further explored and extended. It is shown that for the members of a language, efficiently demonstrating membership in the language releases no additional knowledge. Efficiently demonstrating proofs exist only for non-interactive languages in NP (i.e., P).

Under the assumption that there are no efficient algorithms for finding solutions to NP-complete problems, it is shown that all languages in NP have zero-knowledge proofs. In particular, it is possible to demonstrate that a CNF formula is satisfiable without revealing any other property of the formula, or quadratic residues without revealing a satisfying assignment or properties of a witness.

It is also demonstrated that the underlying proofs are "physical" in nature in the sense that they are verifiable in polynomial time. The main difficulty of an interactive proof for graph isomorphism is a reduction to a graph isomorphism problem in NP and hence an efficient proof was known before for demonstrating that two graphs are not isomorphic.

Categories and Subject Descriptors: C.2.0 [Computer-Communication Networks]: General—data

This work was done while O. Goldwasser was at the Laboratory for Computer Science of MIT, and A. Wigderson was at the Mathematical Science Research Institute of UC Berkeley.

This work was partially supported by an IBM Postdoctoral Fellowship, National Science Foundation grant DCR 860402 and NSF grant DCR 860402, and by the IBM Faculty Development Award.

A preliminary version of this paper appeared in *Proceedings of the 23rd Annual IEEE Symposium on Foundations of Computer Science*, IEEE, New York, 1986, pp. 151-167 (1986).

Authors' addresses: O. Goldwasser, Department of Computer Science, Toronto, Ontario, Canada; Silvio Micali, Laboratory for Computer Science, MIT, Cambridge, MA 02139; A. Wigderson, Institute of Mathematics, Hebrew University, Jerusalem, Israel.

Permission to copy without fee all or part of this material is granted provided that the copies are not made or distributed for direct commercial advantage, the ACM copyright notice and the title of this publication and its date appear, and notice is given that copying is by permission of the Association for Computing Machinery. To copy otherwise, or to republish, requires a fee and/or specific permission.

© 1985 ACM 0897-9131/85/0005-0291 \$08.75

Journal of the Association for Computing Machinery, Vol. 36, No. 5, Sept. 1985, pp. 291-301.

Why: Passwords = (Hard to find) Proofs of Claims

Verifier can be broken into, leaked from, have Malicious Insiders



Prove it !



P and Q s.t. $N=PQ$



Can Alice **prove** to Bob she knows P , Q without **ever** giving them to Bob

Other Proposed Uses

Passwords

Nuclear Disarmaments

DNA identity testing

DNA innocence proving

Validating Transactions on Blockchains preserving privacy and anonymity

Law?

“Public can verify votes of an electronic election were tallied correctly”

input = **Encrypted(Vote)**. Keeping **votes** secret

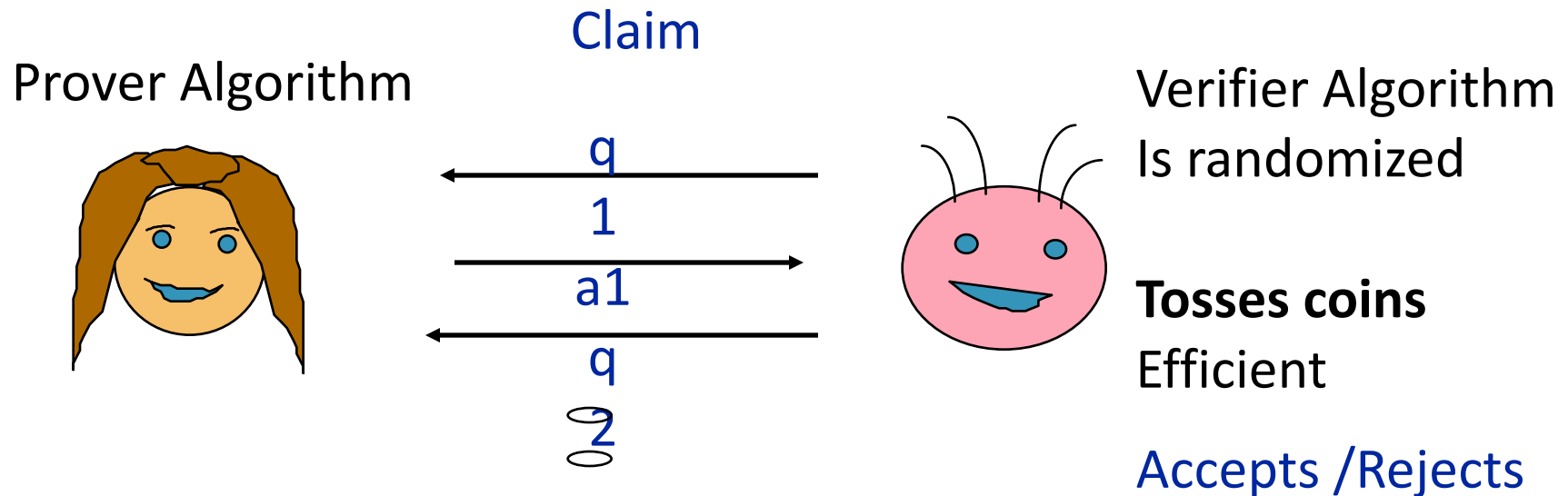
“Public can verify tax return form is compliant with the rules”

without knowing which taxes paid to whom

“Can Verify Whether Documents are Privileged Attorney-Client”

without being exposed to the documents

Interactive and Probabilistically Verifiable Proofs [GMR85]



Completeness: if **Claim is true**, there exists a prover algorithm which will make the verifier accept with

This is what a proof ultimately is!

Soundness: if **Claim is false**, verifier will reject with

probability $> 1 - \text{negligible}$, regardless of prover

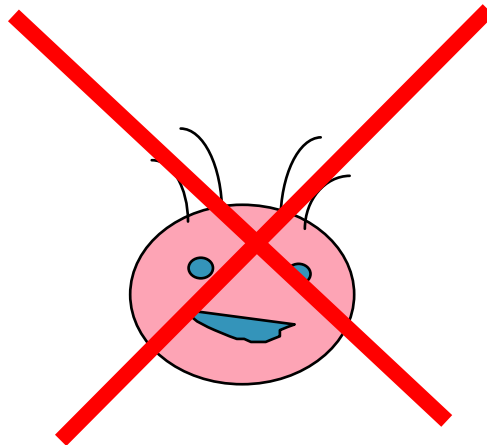
What is Zero Knowledge?

For true claims, for every a verifier

what the verifier can compute after the interaction =

what the verifier could compute before interaction

Adversarial
verifier



More Generally

Can Decouple

“Verifying Correctness”

from

“Knowledge of the proof”

How Would Law Treat

Decoupling

“Verifying Claims”

from

“Knowledge of the facts”

Decisions for Mergers and Acquisitions

Using Zero Knowledge to verify “business facts” to:

- Mitigate the **risks** in disclosure of information for “**due diligence**” when one doesn’t know the motives of the enquirer
- Mitigate the **costs** of disclosure such as suing for expected damages after contract breaches, which might dissuade vindication of legal rights

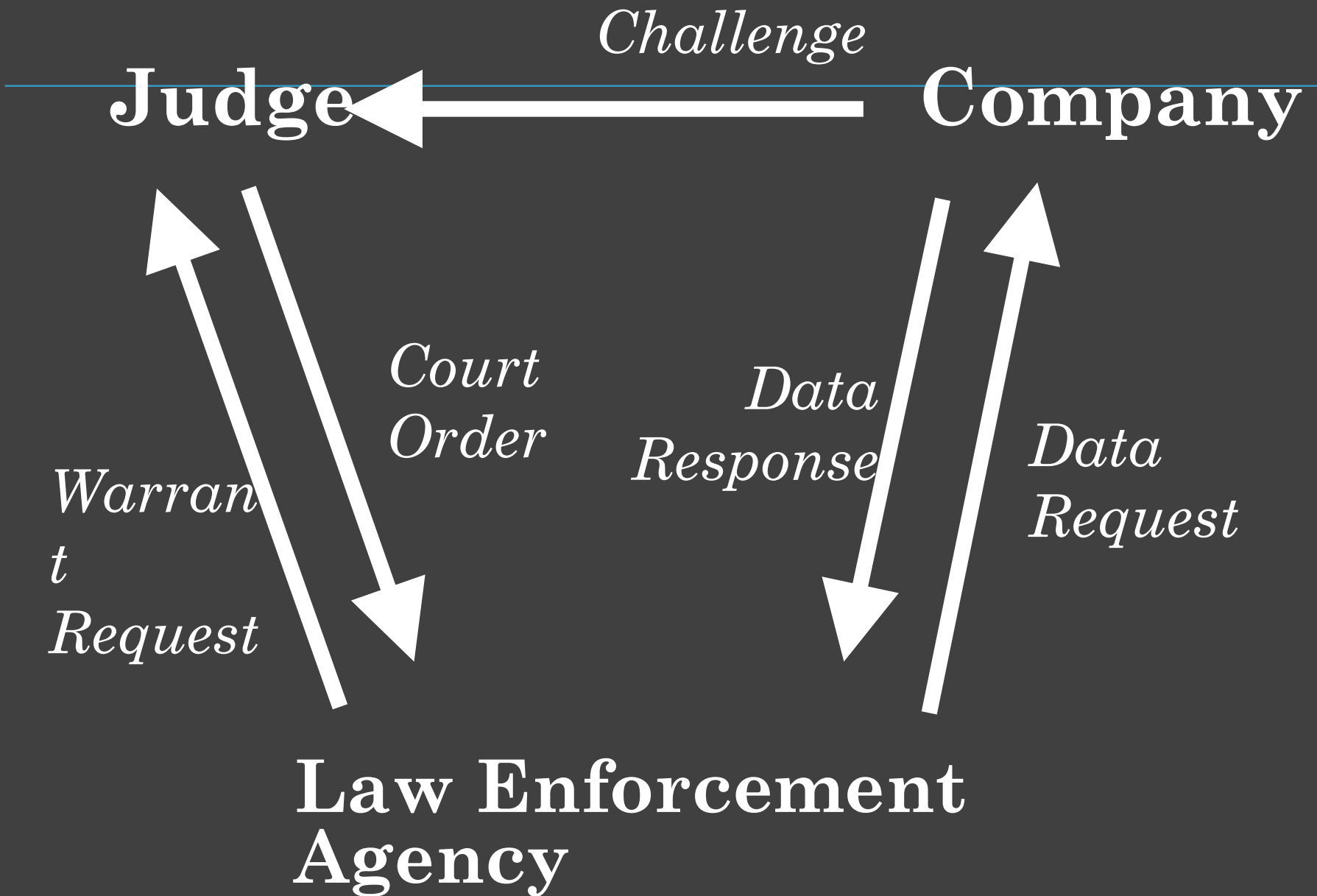
Outline

- ✓ **The Power of Formal Definitions:**
Mathematically (crypto style) define
“The Right to be Forgotten: Discover How to be Compliant”
[GGV2019, in submission]
- ✓ **Potential** of using cryptographic protocols such as ZK and MPC for new and better legal procedures
- **Case in point:** Encryption Debate of Surveillance vs. Government Accountability
“Practical Applicability of Secret Processes”
[FPSGW, USENIX2018]

Government Accountability in Surveillance

Since 1979, [the FISA] court has processed over 28,000 warrant applications and renewals, a rate of nearly one thousand secret cases a year.

Today discuss **the federal docket** that handles tens of thousands of “electronic surveillance warrants” cases every year.



Secrecy is Key

Disclosure of a surveillance order during the course of a criminal investigation would...be self-defeating.

Sealing a case – preventing court records from becoming accessible to the general public.

Gag order – preventing parties involved with the case from mentioning it to others.

Google

Transparency Report Reports ▾ About FAQ

Requests for user information Overview US national security

Requests for user information

Government agencies, courts, and parties in civil litigation regularly ask technology and data. In this report, we disclose information about the number and type of requests we information to shine light on the impact government actions have on our users and the

Twitter Transparency report ▾

Information requests

Information requests - July to December 2017

Apple

Report on Government and Private Party Requests for Customer Information

July 1 - December 31, 2017

Introduction

Apple is very seriously committed the most secure hardware, software have a right to understand how the report provides information regard agencies and private parties from .

Facebook Transparency

STANDARDS ENFORCEMENT ▾ LEGAL REQUESTS ▾ INTERNET DISRUPTIONS

Government Requests for User Data

As part of our ongoing effort to share more information about the requests we have received from governments around the world, Facebook regularly produces this report on government requests for user data to provide

Microsoft Corporate Social Responsibility | More ▾ All Microsoft ▾

Law Enforcement Requests Report



Kudzu in the Courthouse,
Judgments Made in the Shade
(2009)

Gagged, Sealed, & Delivered:
Reforming ECPA's Secret
Docket (2013)

Problems

2. Busy magistrate judges issue hundreds of...orders with literally no appellate guidance

3. The only affected party which might have incentive to object...is never given prior notice of the order.

4. Neither congress nor the public can accurately access the breadth and depth of current electronic surveillance activity.

Judge Smith Proposal

A “**cover sheet**” containing meta data about sealed cases should always be made public

Obvious Tension: Privacy vs. Accountability

Practical Accountability of Secret Processes

[[Usenix 2018, Frankle, Park, Shaar, G and Weitzner](#)]

Propose a System:

Offers greater accountability and privacy is achievable when modern cryptography is brought in: MPC, zero-knowledge proofs, encryption, public ledger

- Demonstrate to the public that each participant performs its role properly and lawfully
- Make public Aware of the extent of Electronic Surveillance

Threat Model

- Judges are honest but forgetful
- Law enforcement agencies might be malicious.
- Companies might be malicious.
- The public might be malicious

Result

MP
C

CIRCUIT

1

CIRCUIT

2

...

DC
CIRCUIT

COURT

1

COURT

2

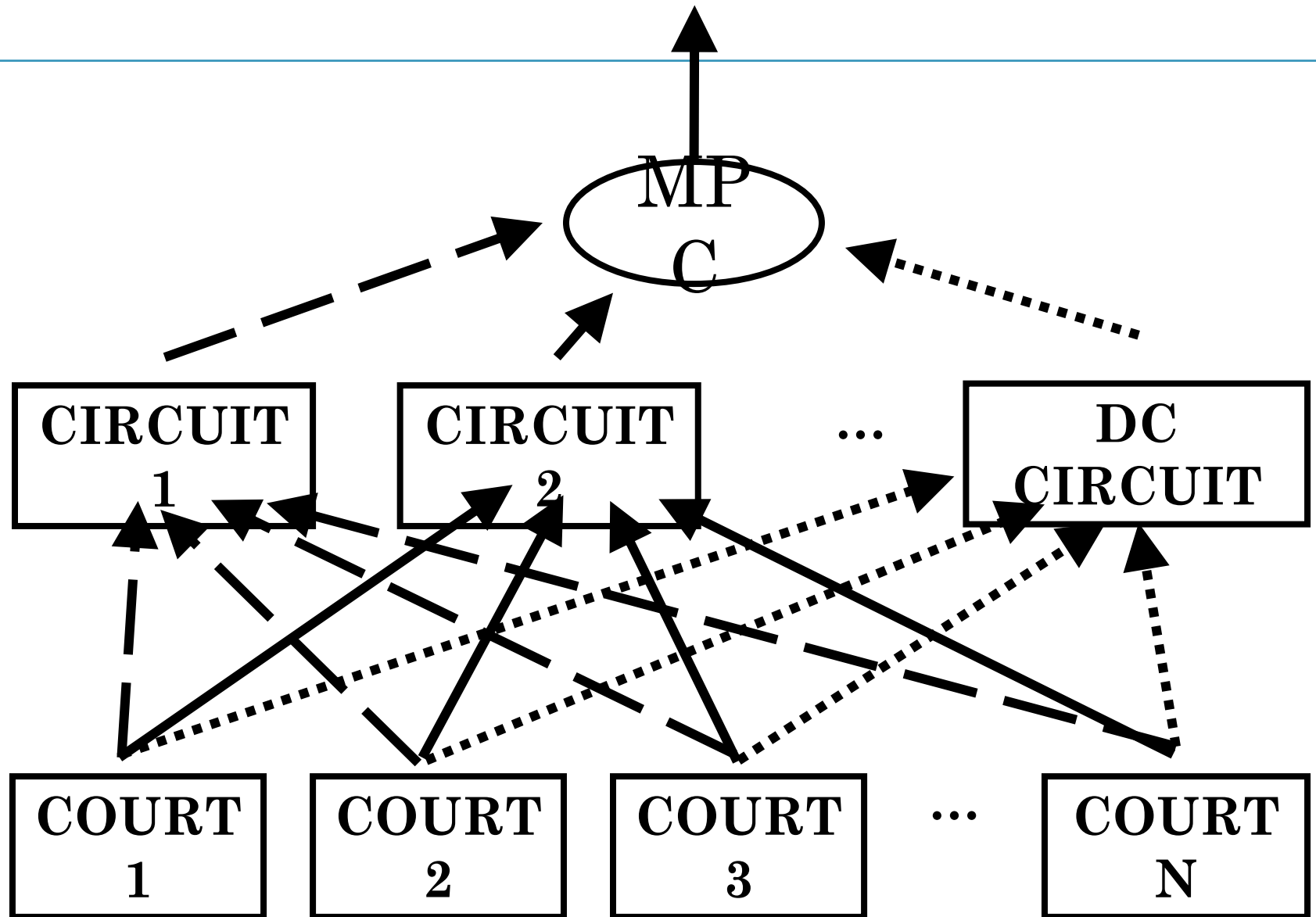
COURT

3

...

COURT

N





My hope is that...court administrators will embrace the possibility of enhancing public oversight while preserving necessary secrecy.

Lessons learned here will... smooth the way towards greater accountability for a broader class of secret information processes, which are a hallmark of our digital age

Quest is **Not** Restricted to Achieving Privacy nor to using Cryptography

Algorithmic Task	Societal Value	Math Formulation	Legal Doctrine
Extract Utility from Data	Privacy	Differential Privacy Multi Party Computation	The right to Privacy
Verify Compliance and Accountability	Privacy	Zero Knowledge Proof	The right to Privacy
Make accurate Predictions and decisions	Fairness	Algorithmic Fairness- several definitions which cannot co-exist	Anti Discrimination
Drive a Vehicle	Safety	Formal Models proposed	Negligence, duty of Care
Moderate online content	Freedom of Speech	Attribute Based Encryption	Copy Right, Fair Use

From “Algorithms and Law” by Elkin-Koren, Feldman, Goldwasser, Talgram-Cohen