Dear Facebook, My Data is None of Your Business

Saikat Guha, Kevin Tang, Paul Francis

Cornell University

WOSN 2008

Privacy in Cloud Computing

- Search history (Google, Yahoo, AOL)
- Emails (Yahoo, Microsoft, Google)
- Documents, Medical history! (Google)
- Photos (Flickr, Google)
- Video watching history (YouTube, Google)
- Web browsing history (DoubleClick, Google)
- Social networks (Facebook, MySpace, Google)

Privacy in Social Networks

Facebook Privacy Policy (Aug 6, 2008)

- All such sharing of information is done **at your own risk.** Please keep in mind that if you disclose personal information in your profile or when posting comments, messages, photos, videos, Marketplace listings or other items, this **information may become publicly available.**
- You understand and acknowledge that, **even after removal, copies of User Content may remain viewable** in cached and archived pages . . . Removed information may **persist in backup copies** for a reasonable period of time but will not be generally available to members of Facebook. .

Privacy in Social Networks

Larry Page on privacy (BBC Interview, May 19, 2008)

"Social networking is the big problem, [. . . when it comes to search data] there's been very little evidence of damage."

Facebook gaffes

- News Feeds (Sep 2006)
- Beacon (Nov 2007)
- Security hole exposes Paris Hilton's pics (Mar 24, 2008)

Trust in Social Networks

1. How many people have an OSN profile?

Trust in Social Networks

1. How many people have an OSN profile?
   - (almost everyone)
2. How many people don't completely trust their OSN provider?

Trust in Social Networks

1. How many people have an OSN profile?
   - (almost everyone)
2. How many people don't completely trust their OSN provider?
   - (more than half)
3. How many people have a minimalist OSN profile?

Trust in Social Networks

1. How many people have an OSN profile?
   - (almost everyone)
2. How many people don't completely trust their OSN provider?
   - (more than half)
3. How many people have a minimalist OSN profile?
   - (more than half)

Privacy and Trust in OSN

- If you trust your OSN provider
  - *Who else* can see your data and at what granularity?
  - How easy for lay users to (mis-)configure?
- If you don't trust your OSN provider
  - Stuck with a minimalist profile

Our Problem

How do you have a rich OSN experience when you don't trust the OSN provider to uphold user privacy?

NOYB: Goals

- User controls who has access to his data
- Arbitrary untrusted OSN provider
  - Cannot see private user data
  - Actively adversarial
  - with reasonable (human) resource limitations
- Instantly usable
  - By individuals or small groups of users
  - Preserves as much OSN functionality as possible

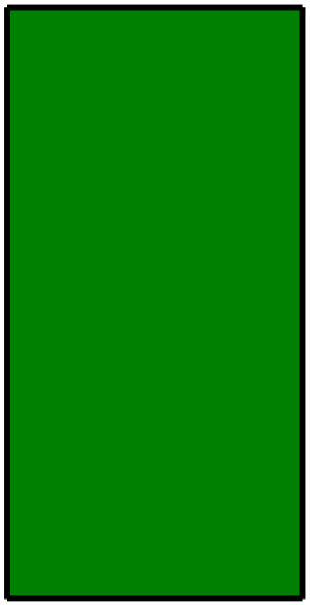
NOYB: Scorecard

- Privacy defined as contextual integrity
- Existence proof: working system
  - Private OSN with rich profiles
  - Arbitrary/adversarial provider
  - Instantly usable by people
- Preserves much OSN functionality
  - Adding new friends
  - Sharing profile and updates with friends
  - ~~Searching for people with similar interests~~
- Experience has reshaped our thinking about how to approach privacy in cloud computing

Privacy as Contextual Integrity

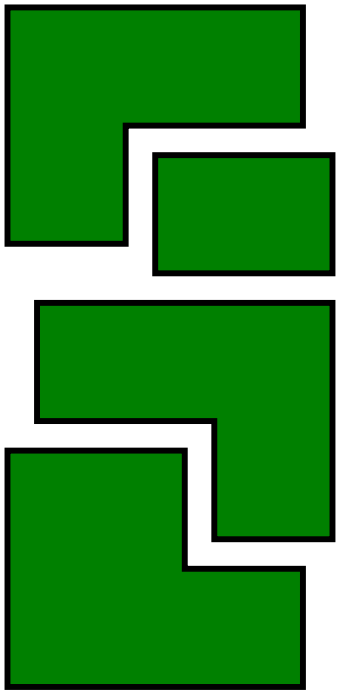
- Profile composed of multiple fields
  - Name, sex
  - Age
  - Relationship status
  - Sexual preference
  - ...
- Out of context, individual fields don't mean much
  - (publicly disclosed in NOYB)
- Ability to recombine fields controls privacy
  - (recombination restricted in NOYB)

NOYB: Profile Scrambling



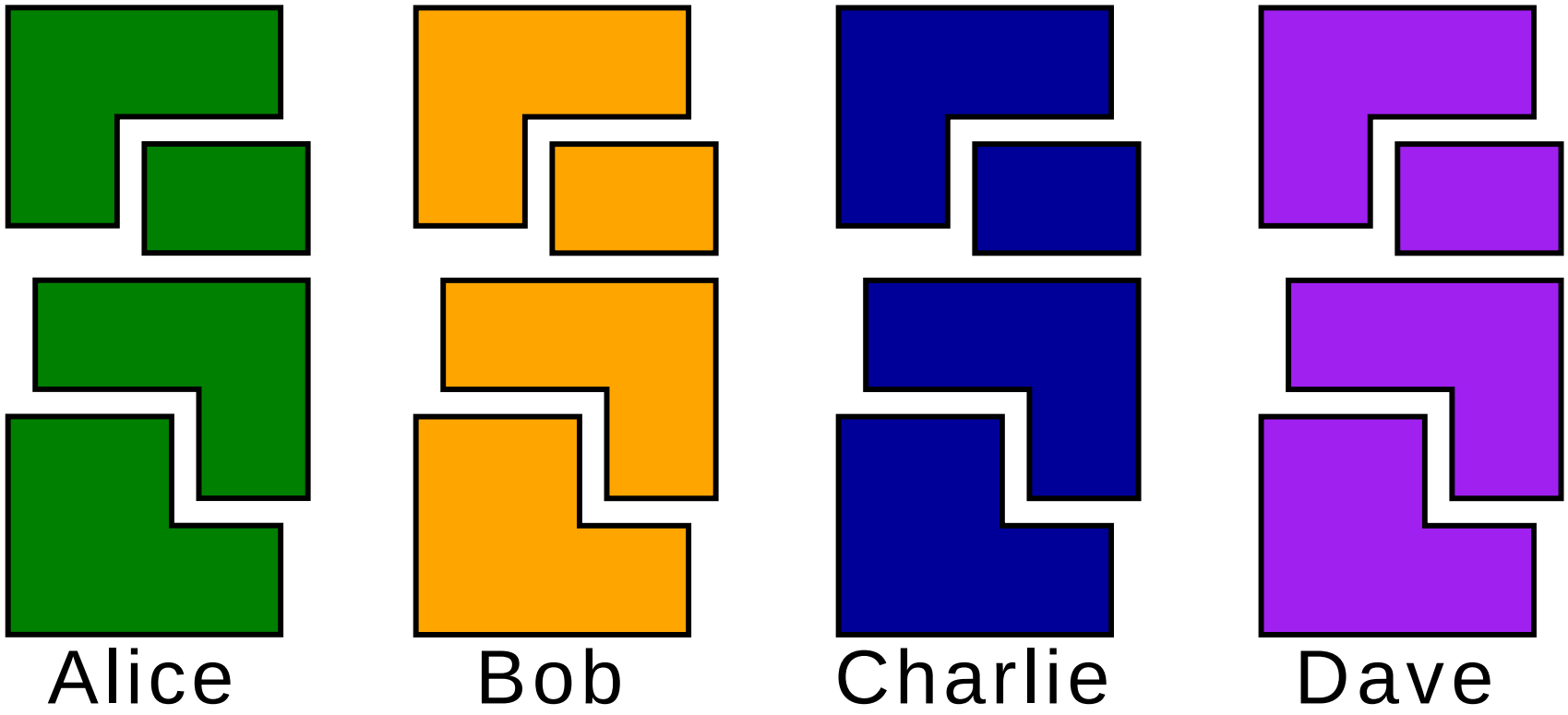
Alice

NOYB: Profile Scrambling

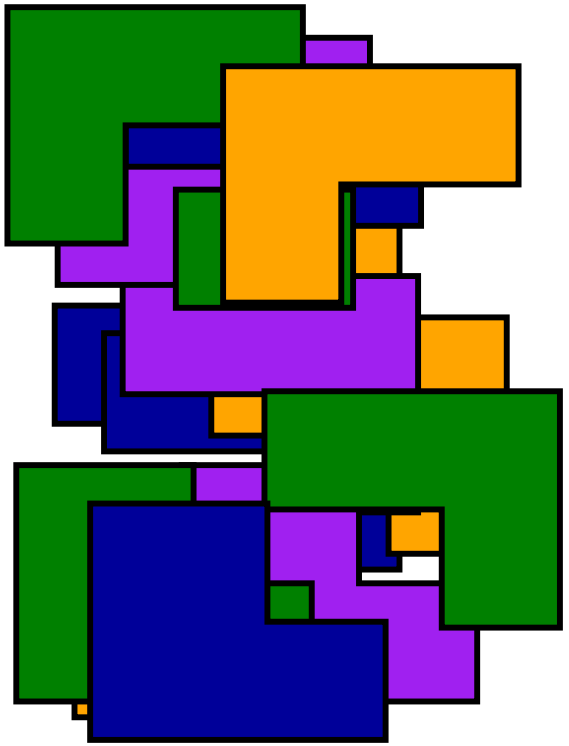


Alice

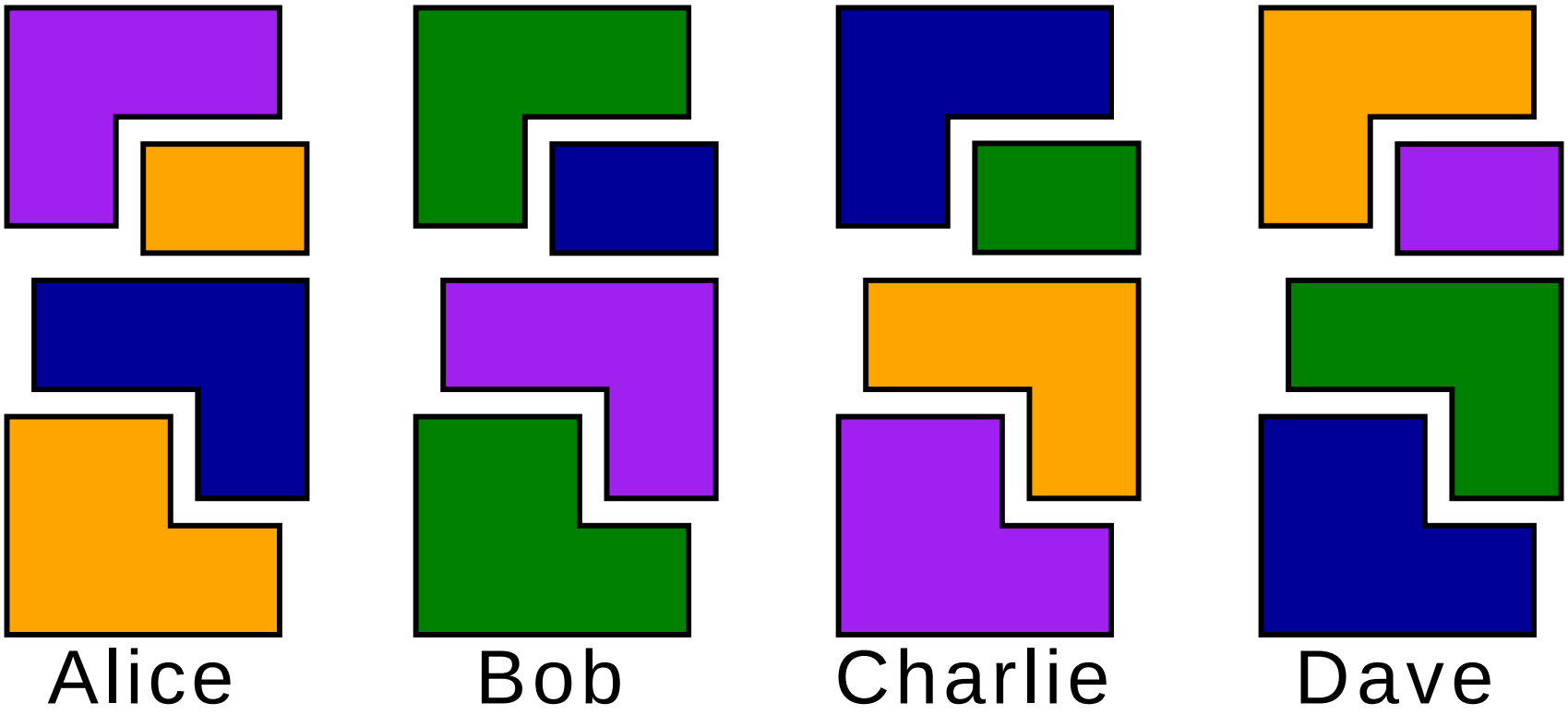
NOYB: Profile Scrambling



NOYB: Profile Scrambling



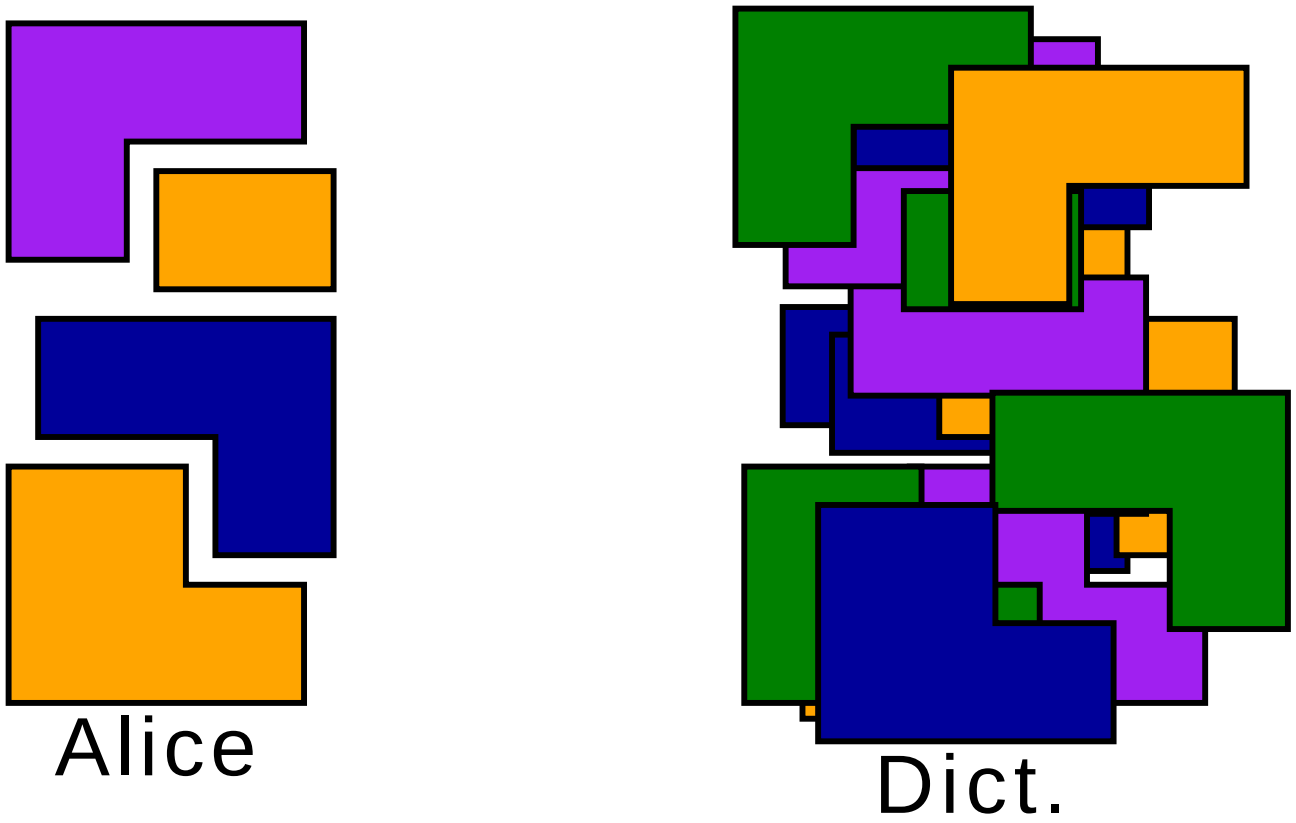
NOYB: Profile Scrambling



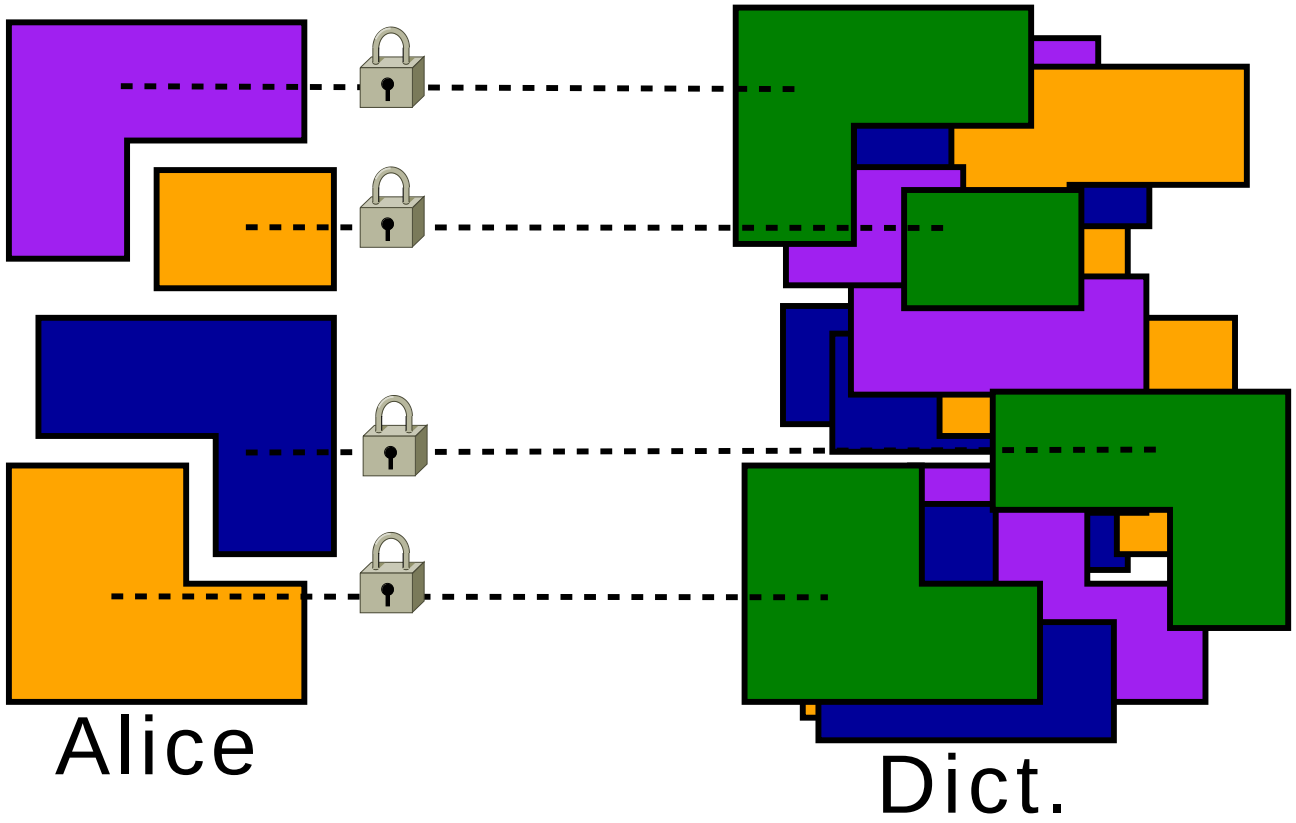
NOYB: Flying Under the Radar

- Scrambled profiles undermine business model (targeted advertising)
  - Facebook may not bother (if few users)
  - But if Facebook does ...
- Hard to *automatically* find NOYB users
  - Piecewise semantically consistent profiles
  - Requires human review (slow)
- PR implications of false accusations
  - NOYB instills reasonable doubt

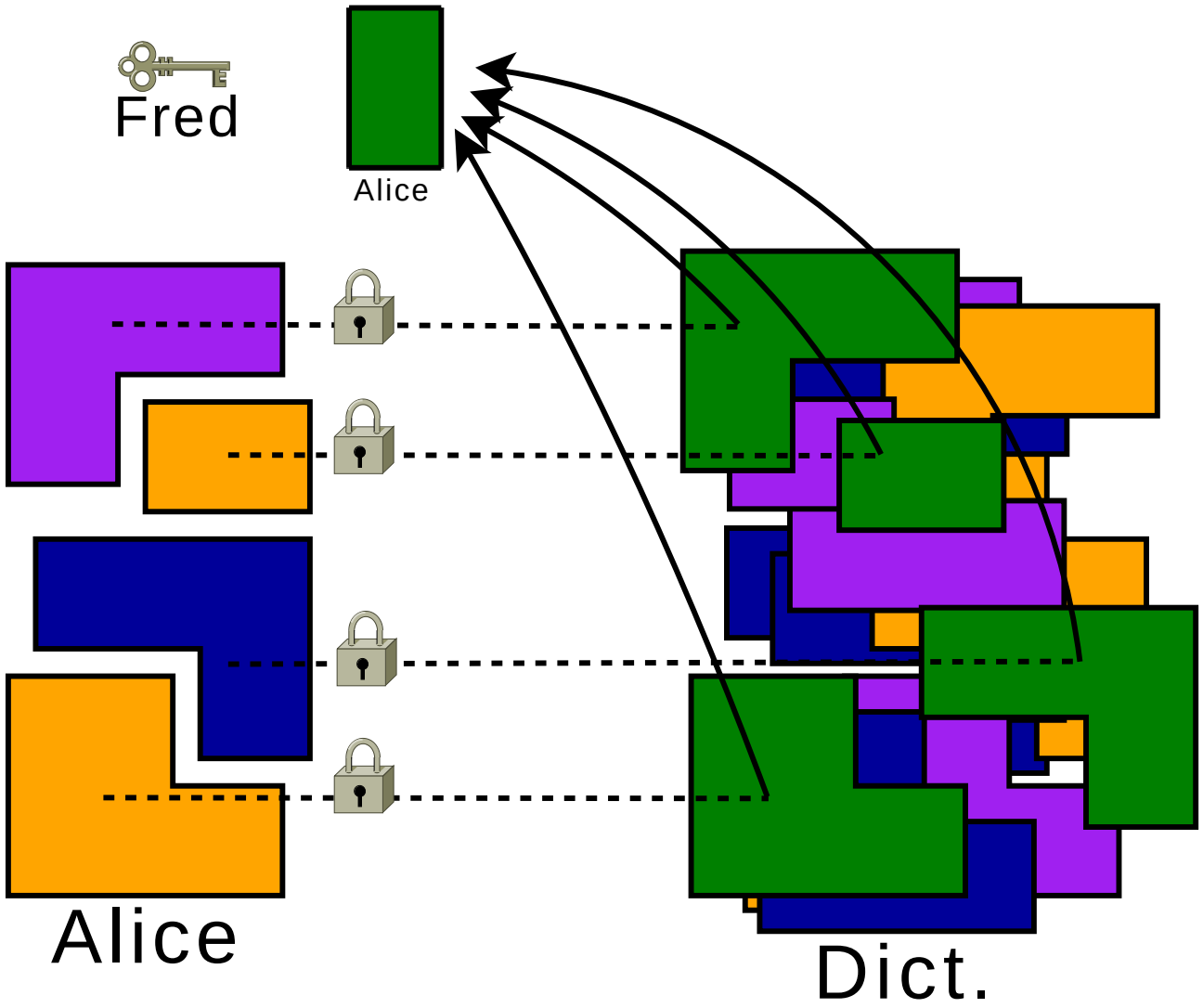
NOYB: Profile Descrambling



NOYB: Profile Descrambling



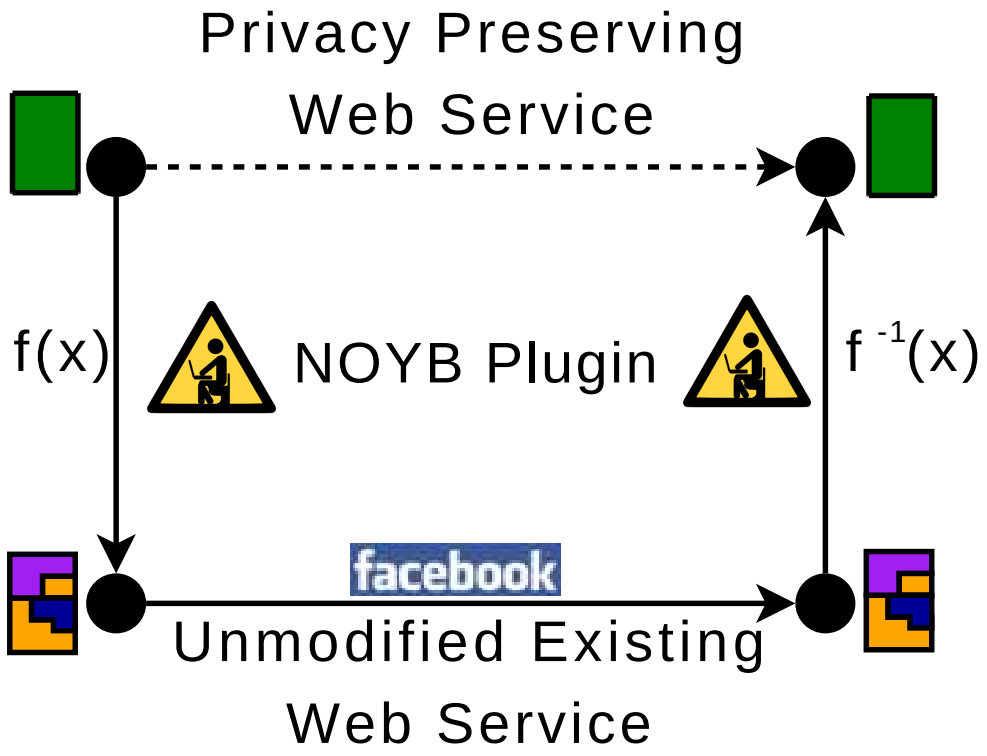
NOYB: Profile Descrambling



NOYB Properties

- Intended for individuals or small groups
  - No buy-in from Facebook
  - Implemented as a browser plugin
- UI: Scramble, Descramble
  - Hides all crypto
  - Can hide key management

NOYB Lessons Learned



- Privacy preserving abstraction function
  - No changes to underlying service
- Complicates system design
- Hard to maintain (as web service changes)

Conclusions

- Privacy preserving abstraction around existing unmodified web services possible
- NOYB provides privacy defined as contextual integrity
  - For individuals and small groups
- Not a long-term strategy
- Ongoing work on architectures that preserve privacy with cooperation from web service (but without trusting them)
  - Provide incentives for this cooperation

Discussion: Privacy in Web Services

How to Ensure User Privacy?

- Trust providers, but checks and balances through
  - Laws and regulation?
  - Market forces?
- Enforce privacy through technological means
  - with or without provider cooperation?
- Role of endhosts in web services?