Anonymity Loves Company: Usability and the network effect

Roger Dingledine, Nick Mathewson
The Free Haven Project

Overview

- We design and deploy anonymity systems.
- Version 1: “You guys are studying this in academia, and we're building them. Please study us.”
- Version 2: “Economics of anonymity are still not considered by (many) researchers.”
- Version 3: “If you're thinking of building an anonymity system...”

Rump session follow-up.

- Yes, usability is an excellent idea. We're working towards that.
- But we're curious about the effects on security as we make progress on usability.
- (Our notion of usability is very broad – e.g. anything that grows the user base.)

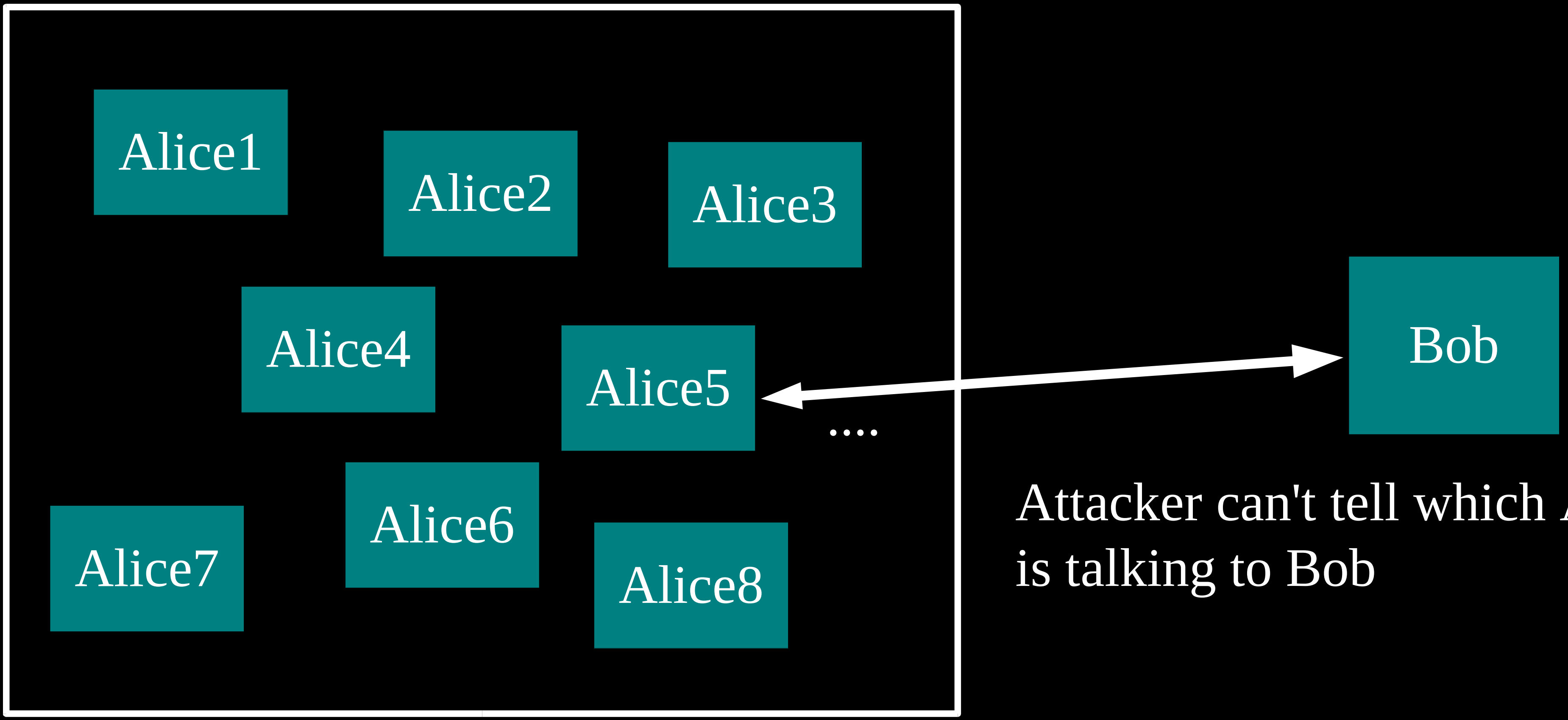
Security is a collaboration

- Suppose two encryption programs:
  - HeavyCrypto is hard to use properly, but more secure if you do.
  - LightCrypto is easier to use, but can't provide as much security.
- Which should you ask your friends to use to send encrypted mail to you? What if you use *both*?
- Security is a collaboration between sender and receiver.

Security affects usability

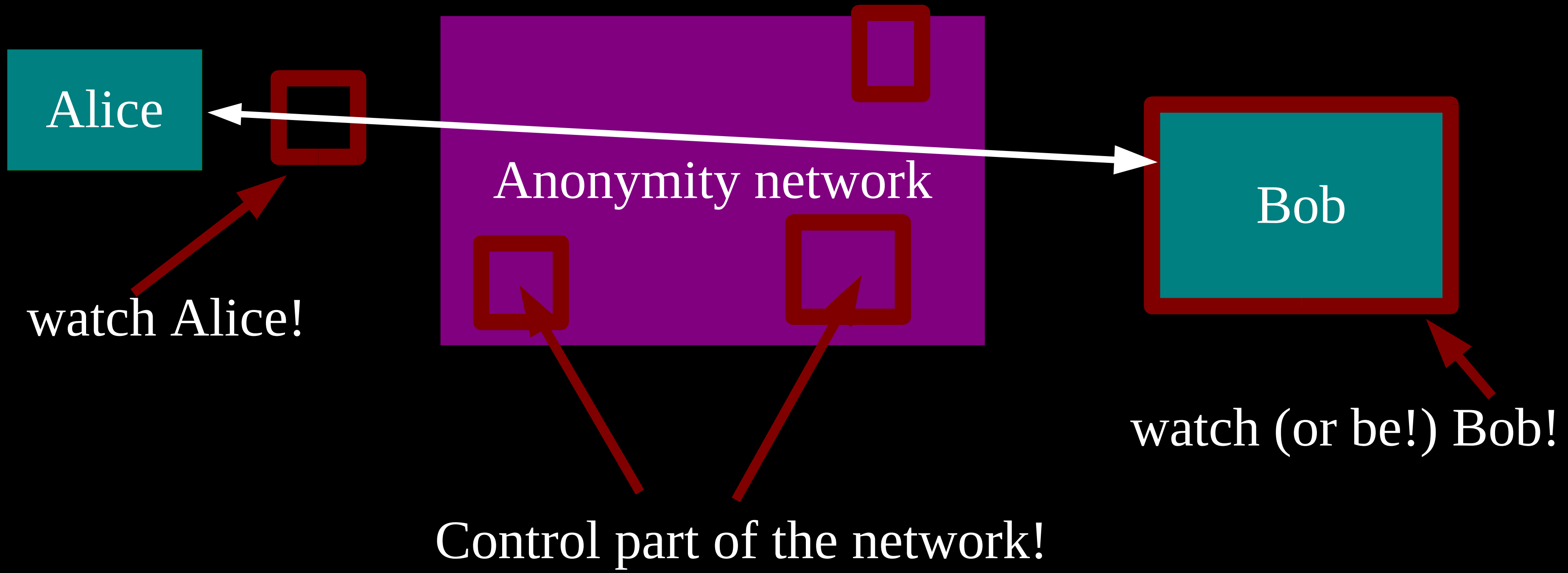
- There are many other cases where usability impacts security (badly labeled off switches, false sense of security, inconvenient security, bad mental models, ...)
- But let's talk about anonymity systems: many people aggregate their traffic to gain security. So now we're talking more than two participants.

Formally: anonymity means indistinguishability within an “anonymity set”



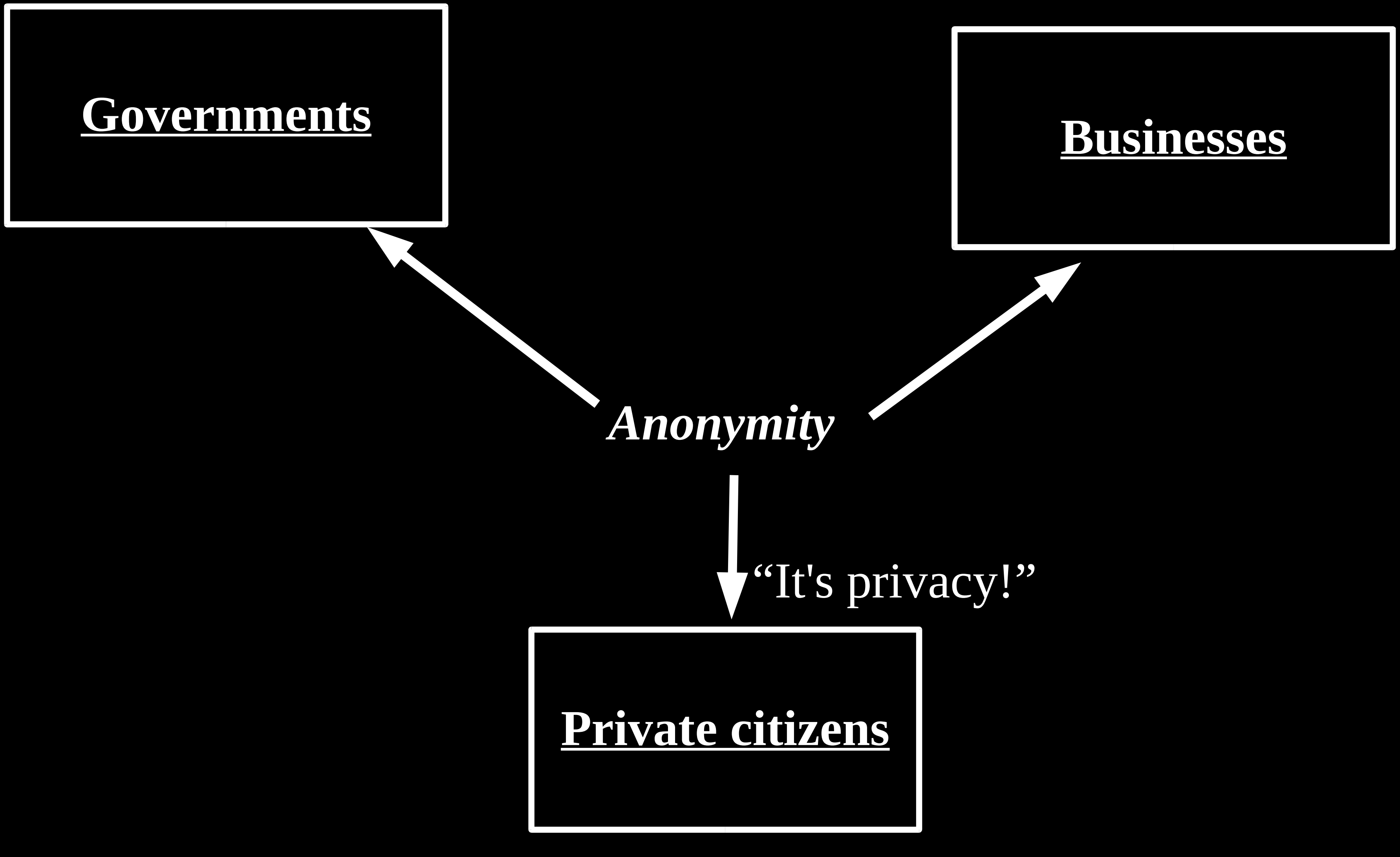
Attacker can't tell which Alice is talking to Bob

We have to make some assumptions about what the attacker can do.



Etc, etc.

Anonymity serves different interests for different user groups.



Governments

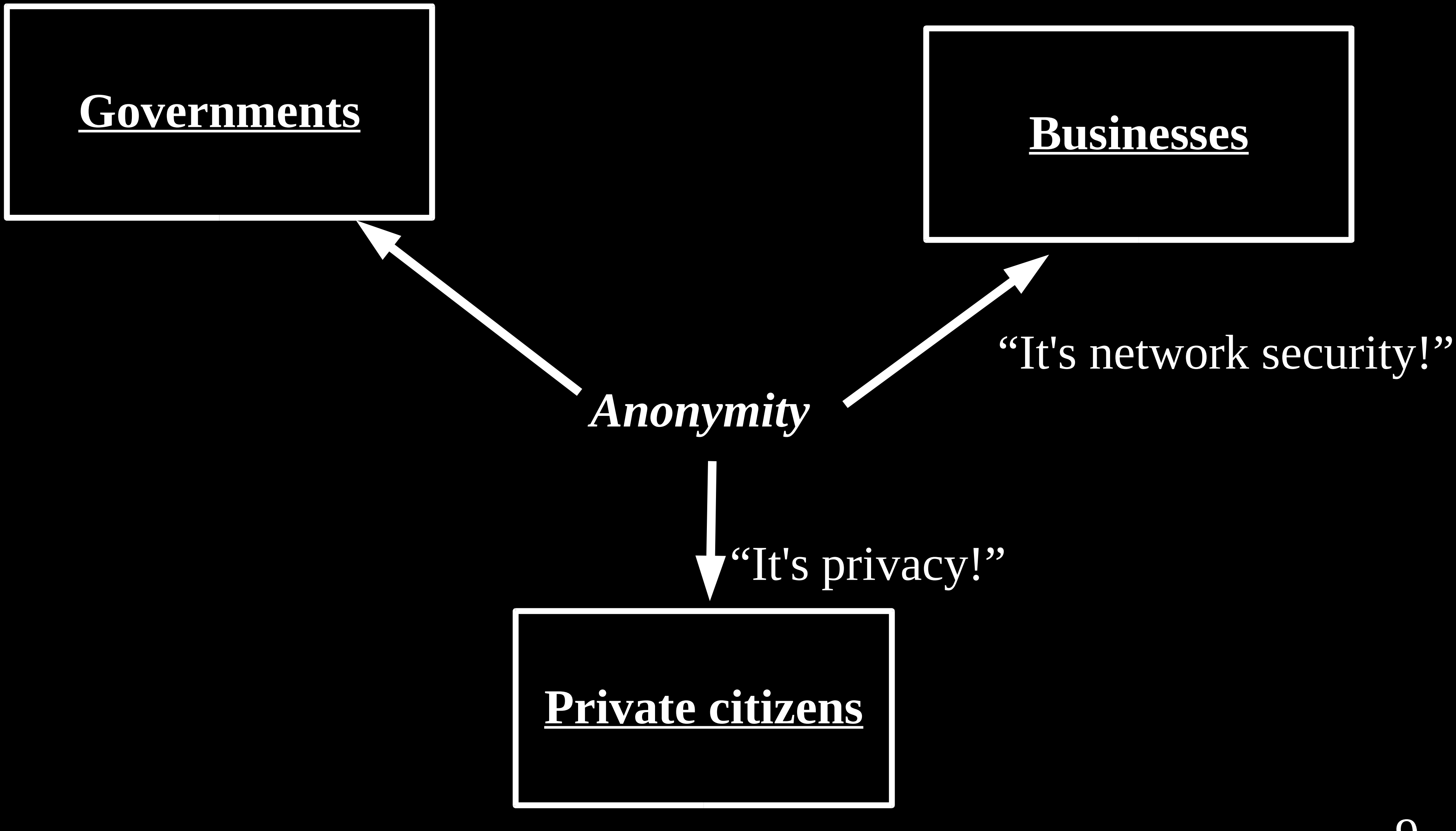
Businesses

Anonymity

“It's privacy!”

Private citizens

Anonymity serves different interests for different user groups.



Governments

Businesses

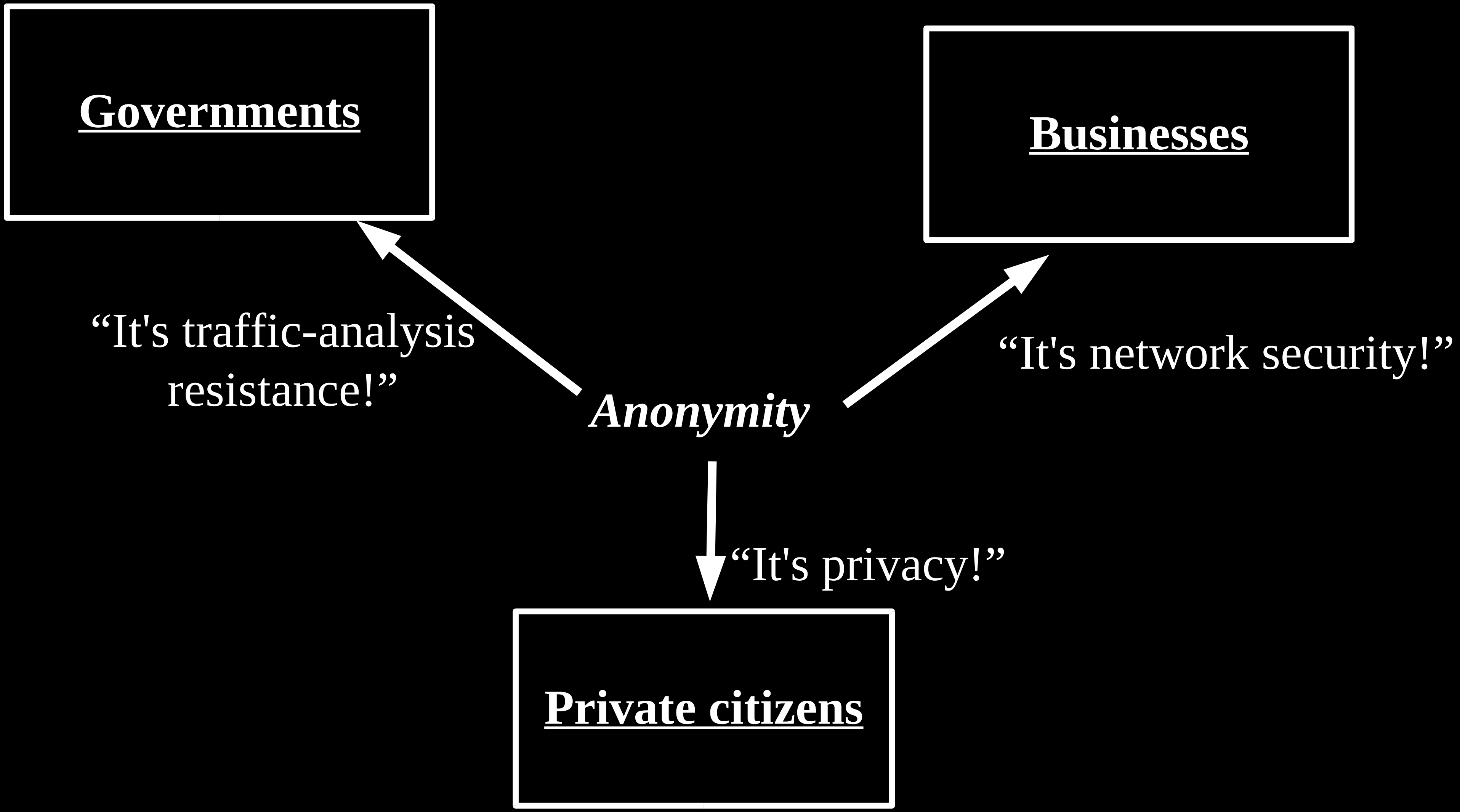
Anonymity

"It's network security!"

"It's privacy!"

Private citizens

Anonymity serves different interests for different user groups.



Governments

Businesses

“It's traffic-analysis resistance!”

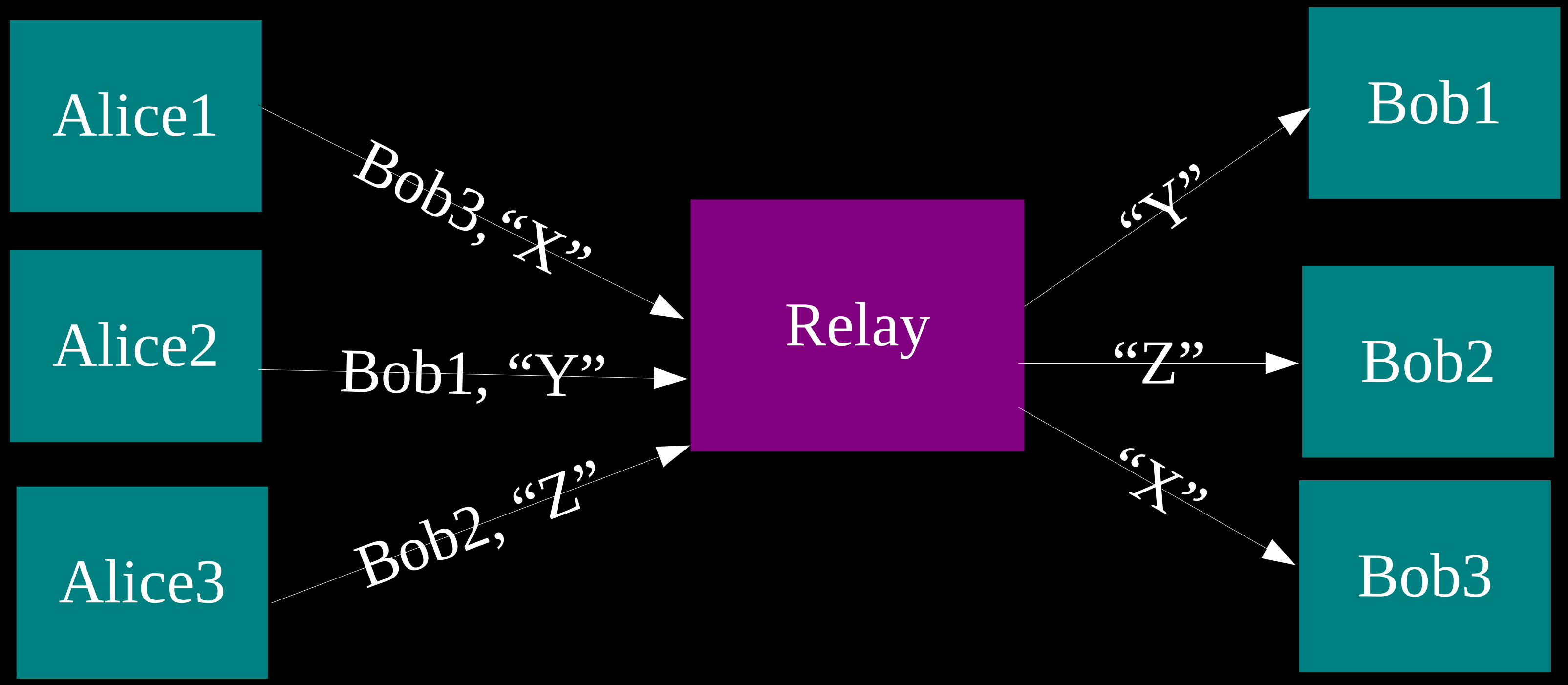
Anonymity

“It's network security!”

“It's privacy!”

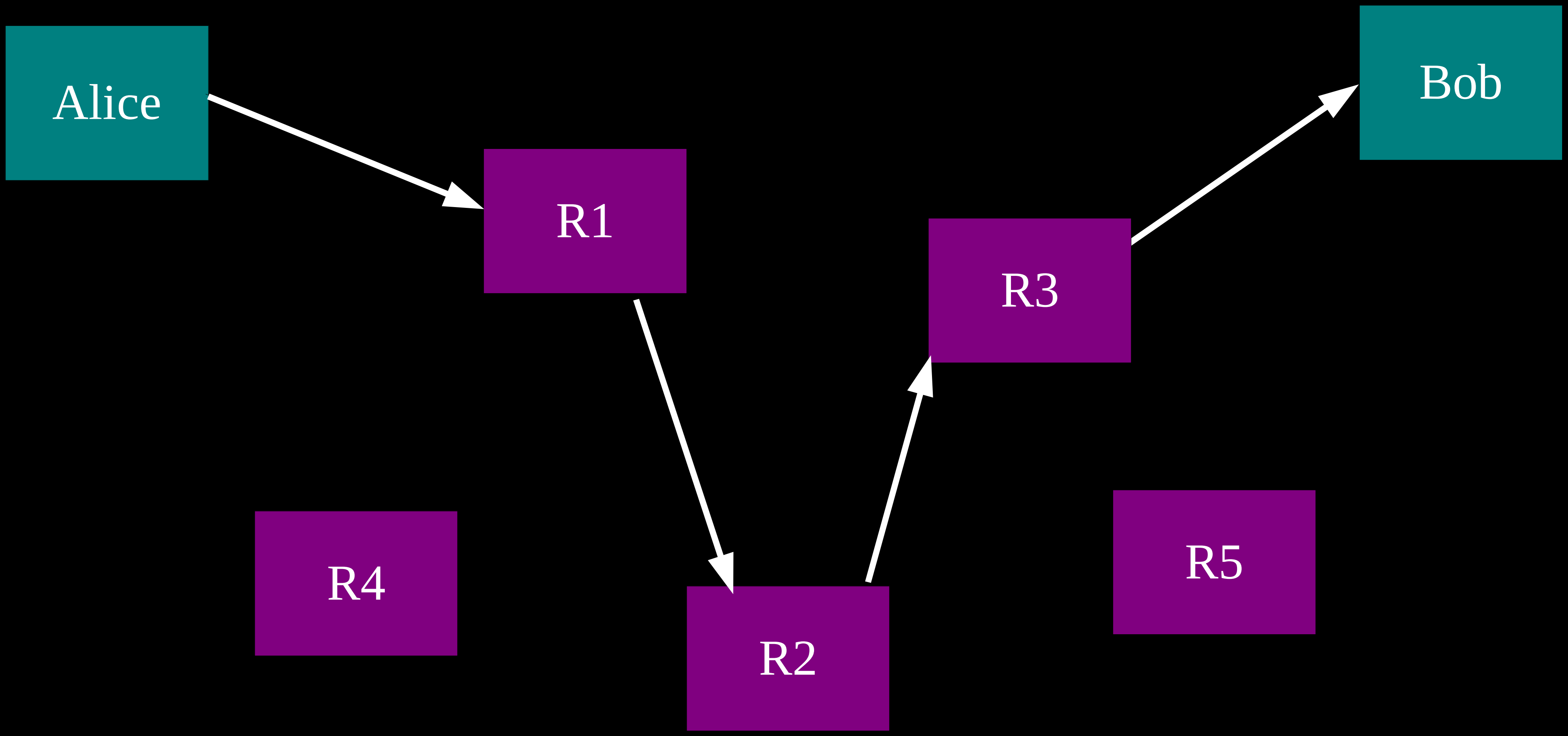
Private citizens

The simplest designs use a single relay to hide connections.



(ex: some commercial proxy providers)

So, add multiple relays so that no single one can betray Alice.



But users need to be behave similarly.

- If two users behave entirely differently, they don't provide cover for each other.
- Some partitioning can be avoided by constructing a better anonymity system (see next workshop).
- But some is inevitable: using different protocols, speaking different languages, etc.
- #1: Users need to consider how usable *others* will find the system, to benefit from a larger anonymity set.

But what about users with different security goals?

- Some designs are high-latency, others low-latency. Protect against different threat models.
- So which should you use if you're flexible?
- High-latency: against strong attackers we're in better shape.
- But if few others choose high-latency, we're weak against both strong and weak attackers!
- #2: Choosing the system with the strongest security model may not get you the best security.

Options can hurt anonymity.

- Options hurt security: users are often not the best people to make security decisions; and non-default configurations don't get tested enough.
- They're even worse for anonymity, since they can splinter the anonymity set. E.g. Type I remailer padding settings.
- #3: Designers must set security parameters.

The default is safer than you think.

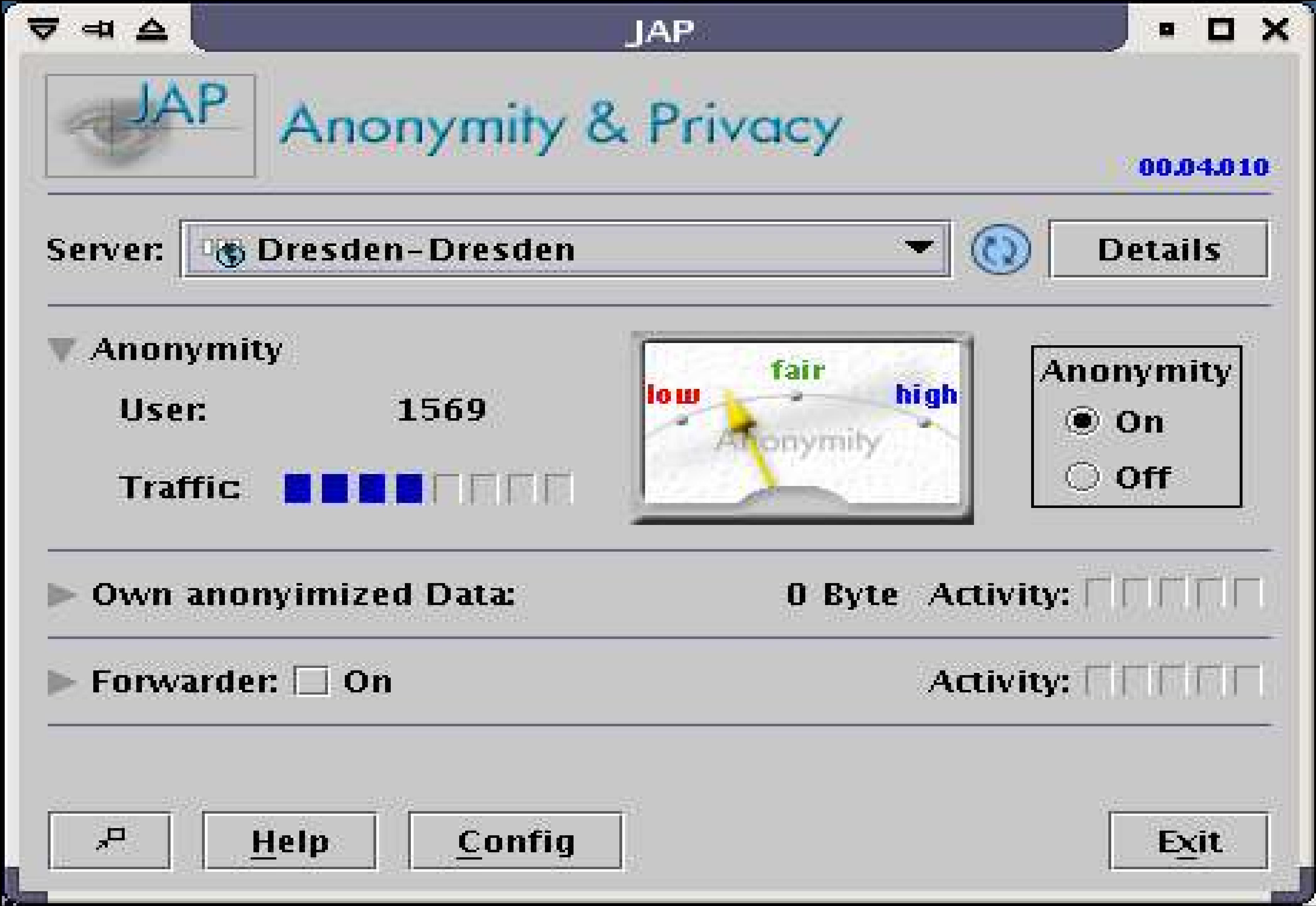
- Even when users' needs genuinely vary, adding options is not necessarily smart.
- In practice, the default will be used by most people, so those who need security should use the default *even when it would not otherwise be their best choice*.
- #4: Design as though the default is the only option.

Convenience vs. Security

- How should Mixminion handle MIME-encoded data? Hard to normalize all possible inputs. Demand that everybody use one mailer?
- Tor path selection: some users want quick paths (one hop), whereas two or three hops seems smarter.
- #5: If you don't support what users want, they'll do it anyway -- insecurely.

Deployment matters too.

- Example: Since Tor is a SOCKS proxy, you need to configure your applications to point to it.
- This is not intuitive for novice users.
- A larger user base doesn't help security-conscious users unless they can configure things right.
- Need to bundle with support tools that configure everything automatically.
- #6: The anonymity questions don't end with designing the protocol. AKA, “ZKS was right.”



Server: Dresden-Dresden

Anonymity

User: 1569

Traffic

Anonymity
● On
○ Off

Own anonyimized Data: 0 Byte Activity:

Forwarder: □ On Activity:

Users want to know what level of security they're getting.

- JAP uses its anonym-o-meter. This is a great idea, but we don't think it's a good metric for low-latency systems.
- Tor doesn't really give users a metric. We don't know what they use.
- #7: Give users a security metric, or they'll infer it from something else.

Bootstrapping

- Most security systems start with high-needs users (early adopters).
- But in anonymity systems, the high-needs users will wait until there's a user base.
- Low-needs users can break the deadlock.
- #8: If you start your system emphasizing security rather than usability, you will never get off the ground.

Perception and Confidence

- Our analysis so far relies on users' accurate perceptions of present and future anonymity set size.
- #9: Expectations themselves can produce trends: the metric is not just usability, but *perceived* usability.
- So marketing can improve security??
- (This is made messier because there aren't good technical metrics to guess the number of users.)

Reputability: the perception of social value based on current users.

- The more cancer survivors on Tor, the better for the human rights activists. The more script kiddies, the worse for the normal users.
- Reputability impacts growth/sustainability of the network. It also dictates how many strong attackers are attracted.
- #10: Reputability affects anonymity, and a network's reputation can be established early.

Anonymity's network effect vs. other network effects.

- Say I have a ham radio and a telephone. I lose nothing other than my investment in the ham radio. Same with VHS and Beta.
- Whereas if I participate in a secure and an insecure anonymity network, even if I make all my decisions well, I still am worse off.
- People use number of customers as a signal -- "But if more customers actually improve the quality of the burger..."

Conclusions

- Bad loop: unusability means insecurity.
- Good loop: usability means security.
- We can't just wait to build the most usable and most secure system: people are going to take their actions anyway, on less safe systems.