

Privacy vs. Data: Business Models in the digital, mobile Economy

Lecture 9 + 10
Privacy & Privacy Protection

WS 2011/2012

Dr. Andreas Albers
www.m-chair.net



- What is Privacy?
- Data Protection Directives and Laws
- Technical Data Protection
- General Requirements for Privacy
- Privacy by Design

What is privacy?

- Privacy (from latin: separated from the rest, deprived of something, esp. office, participation in the government", from privo "to deprive")
 - Some definitions ...
 - „... right to be left alone” [Warrend and Brandeis, 1890]
 - “... right not to be annoyed” [Varian, 1996]
 - But there are many more ... and privacy is a very complex, multi-disciplinary concept ...
 - Technical, economic, legal, socio-economic, philosophic aspects
- So, no working definition here ...



- Societal perspective
 - Foundation of Democracy
 - Freedom of Speech
- Individual perspective
 - Free personal development
 - Ownership of personal data of any kind
- But in an information society, it takes effort for individuals to protect their privacy



Why privacy? Parallels to political instable regions of the world?

- Political instable regions of the world
 - Enterprises hesitate to invest in their business because they are afraid of losing it again soon
- Individuals without privacy
 - Individual hesitate to develop personally because they are afraid of being observed/surveilled and may experience consequences from this act

- Offline Privacy

- In the offline world individuals are able to maintain their privacy intuitively



- Online Privacy

- In the online world, privacy
 - has to be maintained through complex privacy settings or identity management
 - often cannot be maintained at all by individuals because personal data is collected even without their knowledge



- The Internet does not forget or is sometimes not allowed to do so (data retention)
- The Internet allows to easily connect social roles or partial identities, which would have been separated in the offline world
- Profiling is easy and can be done automatically
- managing personal information is complex and has to be done manually



- Data Protection (EU / Germany)
- Technical Data Protection
- Privacy by Design

- Identity Management (in Lecture 11)



- What is Privacy?
- Data Protection Directives and Laws
- Technical Data Protection
- General Requirements for Privacy
- Privacy by Design

- **Definition**

Measures for the protection of stored and transferred personal data against manipulation or misuse; Federal Data Protection Act in place since 1978 (amendment in 1990).

- Originally for the protection of the citizen against governmental institutions.
- Businesses are regulated with regard to special aspects (telecommunications, medicine) of data protection.
- Increased need for regulation due to the use of information technology (data warehouses, globalisation of information processing).

- **Data minimisation:**

The service should be offered with a minimum of needed data.

- **Information of data subject:**

The person, whose data is being stored, should know what has been stored.

- **Acceptance not without consent:**

The data subject is to be asked in advance.

- Both terms are related but not synonymous and have many definitions.
- 2 popular ones:
 - **Data protection** is the protection from harmful and unsolicited usage of data linked to the personal sphere of a person.
 - **Privacy** is the right to be left alone, e.g. to be unwatched or anonymous [Source: Warren and Brandeis (1890)].
- More work needed on a complete understanding of privacy
- Nevertheless the topic is important, as one can see from related incidents and activities to address the issue.

- Data Protection Directive (Directive 95/46/EC)
 - Directive on the protection of individuals with regard to the processing of personal data and on the free movement of such data
- Directive on Privacy and Electronic Communications (Directive 2002/58)
 - Directive on Privacy and Electronic Communications with regard to data retention, spam and cookies





1. **Intention and notification:** The processing of personal data must be reported in advance to a Data Protection Authority.
2. **Transparency:** The person involved must be able to see who is processing her data for what purpose.
3. **Finality principle:** Personal data may only be collected and processed for specific, explicit and legitimate purposes.
4. **Legitimate grounds of processing:** The processing of personal data must be based on a foundation referred to in legislation, such as permission, agreement, and such.
5. **Quality:** Personal data must be as correct and as accurate as possible

[Blarkom and Borking, 2003]



6. **Data subject's rights:** The parties involved have the right to take cognisance of and to update their data as well as the right to raise objections.
7. **Processing by a processor:** This rule states that, with the transfer of personal data to a processor, the rights of the data subject remain unaffected and that all restrictions equally apply to the processor.
8. **Security:** A controller must take all meaningful and possible measures for guarding the personal data.
9. **Transfer of personal data outside the EU:** The traffic of personal data is permitted only if that country offers adequate protection.

Source: Blarckom and Borking (2003)

Germany: Federally organised data protection



- Responsibility in Germany:
Federal Commissioner for Data Protection and
Freedom of Information (BfDI)
- Each state in Germany has its “Länder” Data
Protection Commissioner.
 - Specialisation on certain fields, e.g. in Schleswig-
Holstein (ICPP) on Privacy in the Internet
- **Additionally:**
Data protection commissioners within governmental
administration and within companies

The origin of data protection in Germany?



- The term “Privacy” (‘the right to be left alone’) originates from [Warren and Brandeis, 1890].
- Data protection in Germany (“Datenschutz”) originates from concerns over too much information und power in the hands of large (governmental” institutions (“Big Brother”).
- Nowadays Data protection and Privacy in Germany are based on the right of informational self determination derived from the constitution in the “Volkszählungsurteil“ [BVG 1983]).
- Germany has one of the most advanced infrastructures for Privacy but still no established German language term for Privacy beyond the (misleading “Datenschutz”).
- Some (more or less established) related terms are:
 - Privatheit
 - Privatsphäre
 - Schutz der Privatsphäre

- 27th International Conference of Data Protection and Privacy Commissioners
- 2005-09-14/16 in Montreux, Switzerland
- “The protection of personal data and privacy in a globalised world: a universal right respecting diversities” [Source: ICDPPC (2005)]
- Agreement on 11 principles by participating data protection and privacy commissioners

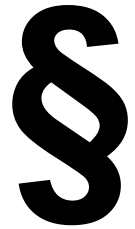
- Lawful and fair data collection and processing,
- Accuracy,
- Purpose-specification and -limitation,
- Proportionality,
- Transparency,
- Individual participation and in particular the guarantee of the right of access of the person concerned,
- Non-discrimination,
- Data security,
- Responsibility,
- Independent supervision and legal sanction,
- Adequate level of protection in case of transborder flows of personal data.

- Users want to keep their personal data under their control.
- Service providers want to use the customers' data for commercial purposes (e.g. customer profiles).
- The legislator demands:
 - Data protection on the one hand,
 - Surveillance and retention of data on the other hand.
 - Conflicts between expectations and regulations often arise.



Regulation is “alive” and constantly demands new decisions.

Law alone is not sufficient



- The increased usage of IT systems and networks leads to
 - huge amounts of data
 - easily searchable data
 - automatic analysis
 - and knowledge extraction

- Data protection / Privacy law alone not sufficient
 - Not all processing can be controlled (e.g. every network node).
 - Deliberate breaking and bending of law (different legislations on the internet)
 - Economic pressure can force customers to give consent to almost any kind of ‘privacy’ policy (e.g. selling privacy for “peanuts”).

- Slow pace of privacy self-regulation in the US, Focus on self-help
 - Self regulation by sustaining user ignorance
 - Enforcing norms may violate anti-trust.
 - Being a good actor (e.g. by exposing privacy practices) increases liability.
 - Legal compliance and related business processes (deemed) expensive

Source: Reagle (1998); SelfReg (1999); Bell (2001); Hoofnagle (2005)

- ⇒ Technical Privacy Protection
- ⇒ Standardisation

- What is Privacy?
- Data Protection Directives and Laws
- Technical Data Protection
- General Requirements for Privacy
- Privacy by Design



- Individuals
 - want to control the amount of identity information visible from the outside.
 - consider what personal information they reveal to whom.
- Typical protection techniques are:
 - Anonymization and identity management tools
 - Spontaneous switching between different levels of anonymity and pseudonymity depending on the context

- The Anonymizer

www.anonymizer.com

Anonymizer®

- Mixmaster – Anonymous Remailer

<http://mixmaster.sourceforge.net>

- Java Anonymous Proxy (JAP)

<http://anon.inf.tu-dresden.de>

JAP Anonymity & Privacy

- Tor Network

<http://tor.eff.org/>



- Cookie Cooker

www.cookiecooker.de

CookieCooker

- P3P - Platform for Privacy Preferences

www.w3.org/P3P

- Idemix

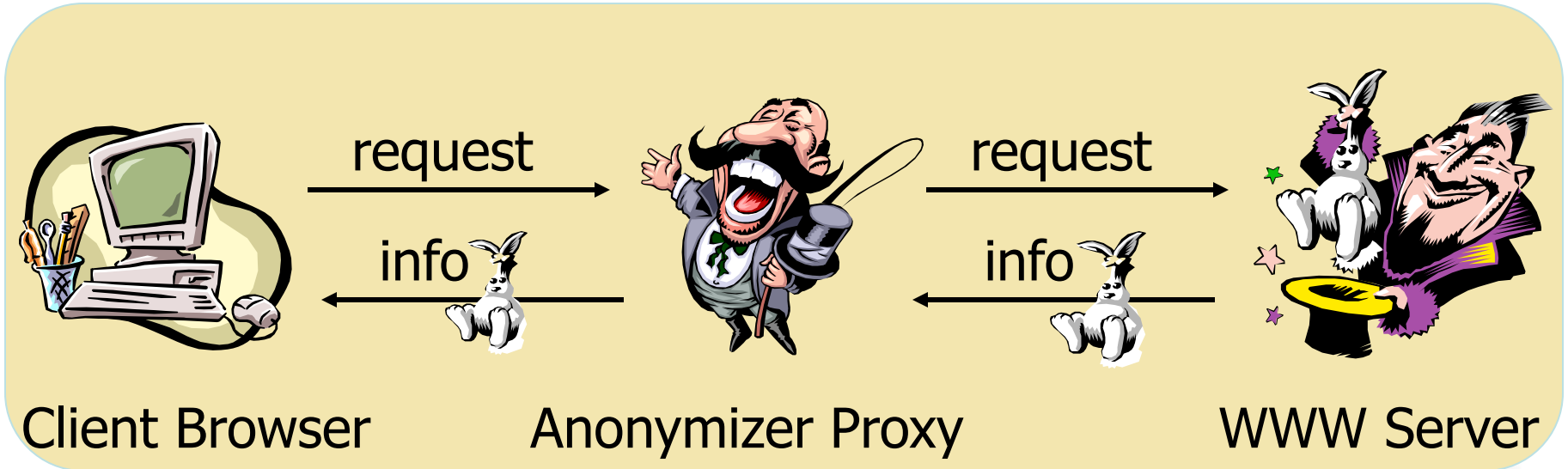
www.zurich.ibm.com/security/idemix

idemix 

- Online Tracking Protection

- DoNotTrack
- IE Tracking Protection

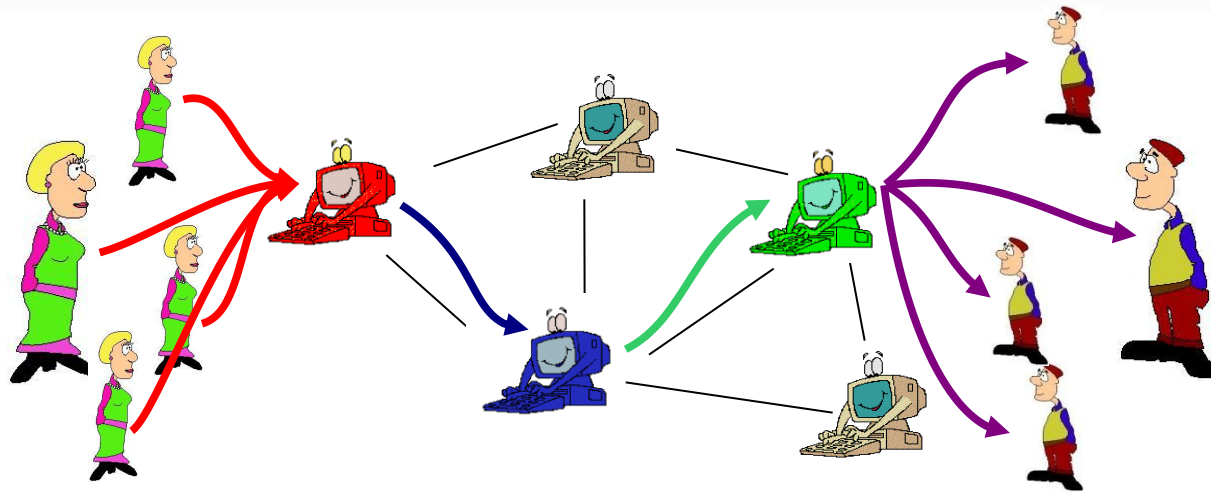




www.anonymizer.com

- ↑ Client (anonymity) is protected in an “anonymity set” of all possible proxy clients.
- ↓ Anonymizer learns about client’s activities / interests.
- ↓ No protection against attackers with global view.

Mixes and Onion Routing

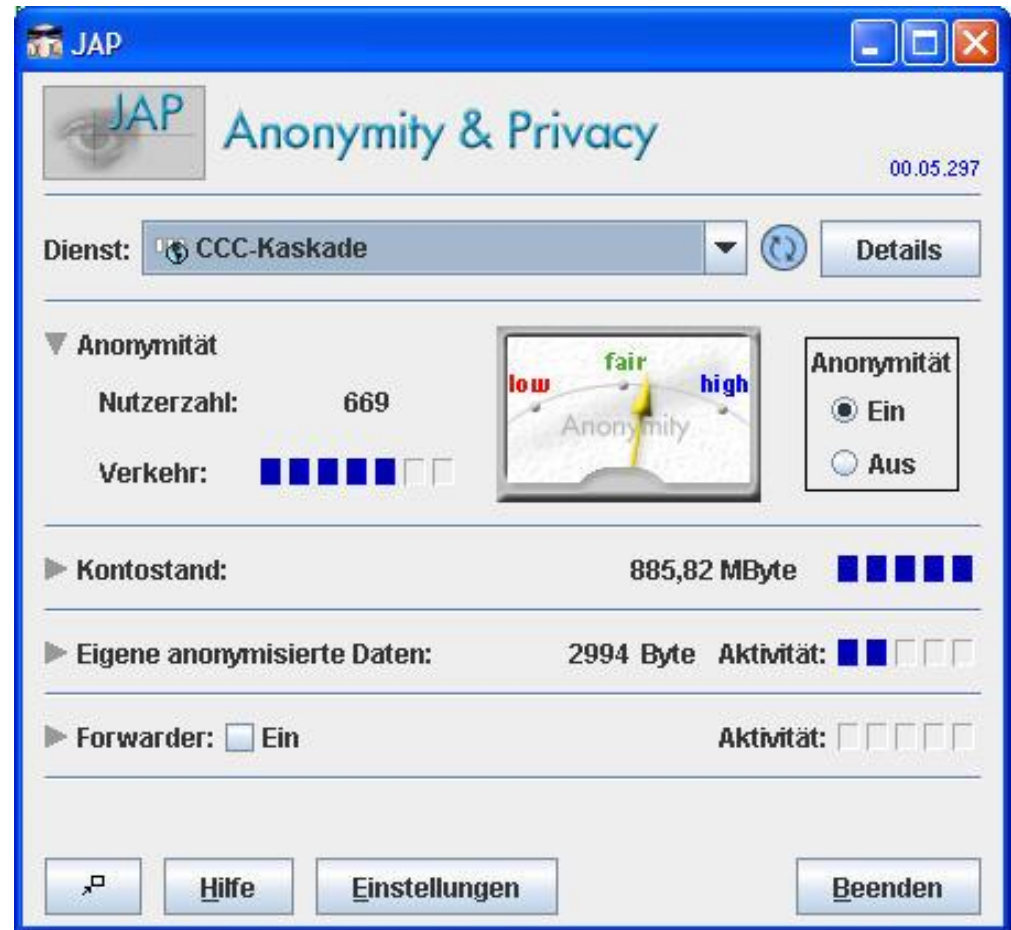


- *Communication is anonymised by multiple mix servers, also called onion routers.*
 - *Both onion routing and JAP are based on the same Mix concept.*

Java Anonymity Proxy (JAP)

- Users can choose between multiple mix-cascades.
- Number of active users is a heuristic for level of anonymity achieved.
- Current version does not achieve security against a global attacker but can protect against local attackers
 - your boss
 - your provider
 - operator of a mix

<http://anon.inf.tu-dresden.de>

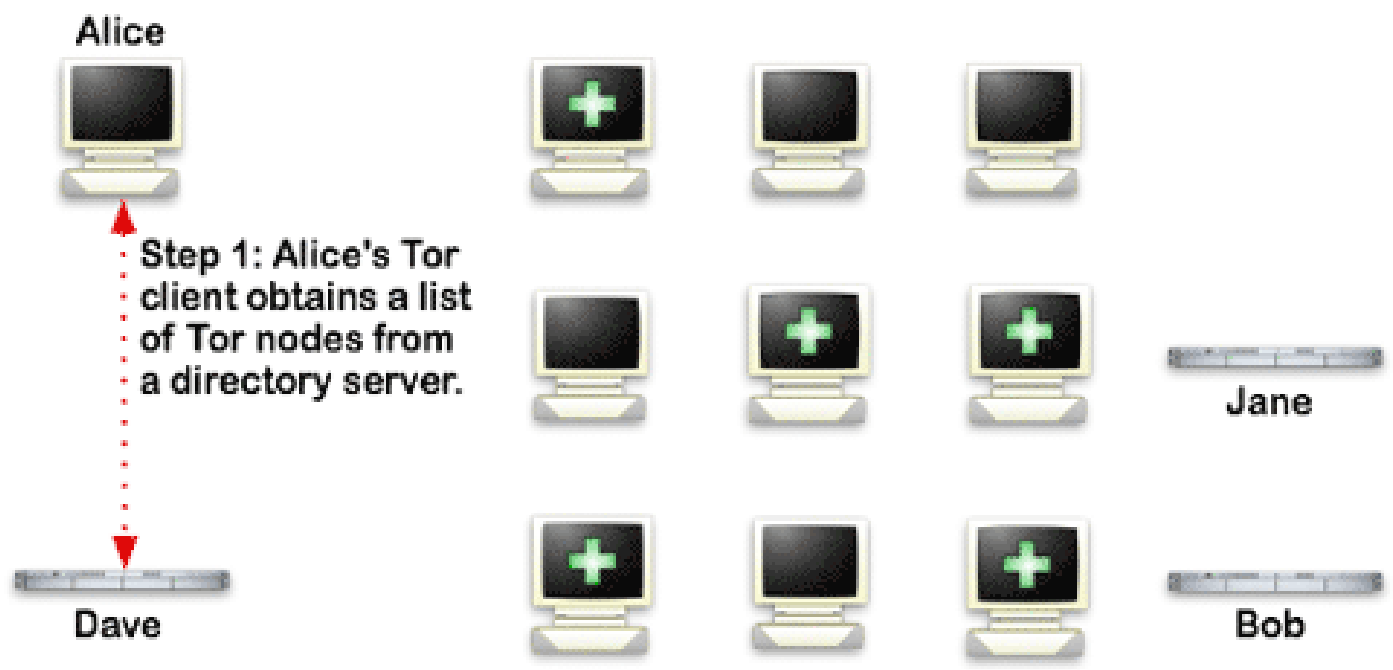


- Tor is a network of virtual tunnels that allows people and groups to improve their privacy and security on the Internet.
- Distributed anonymous network
- Tor allows users to change circuits during sessions
 - Aims to minimize linkability of actions
- May be affected by the data retention directive (as well as JAP)
 - Anonymity and data logs?

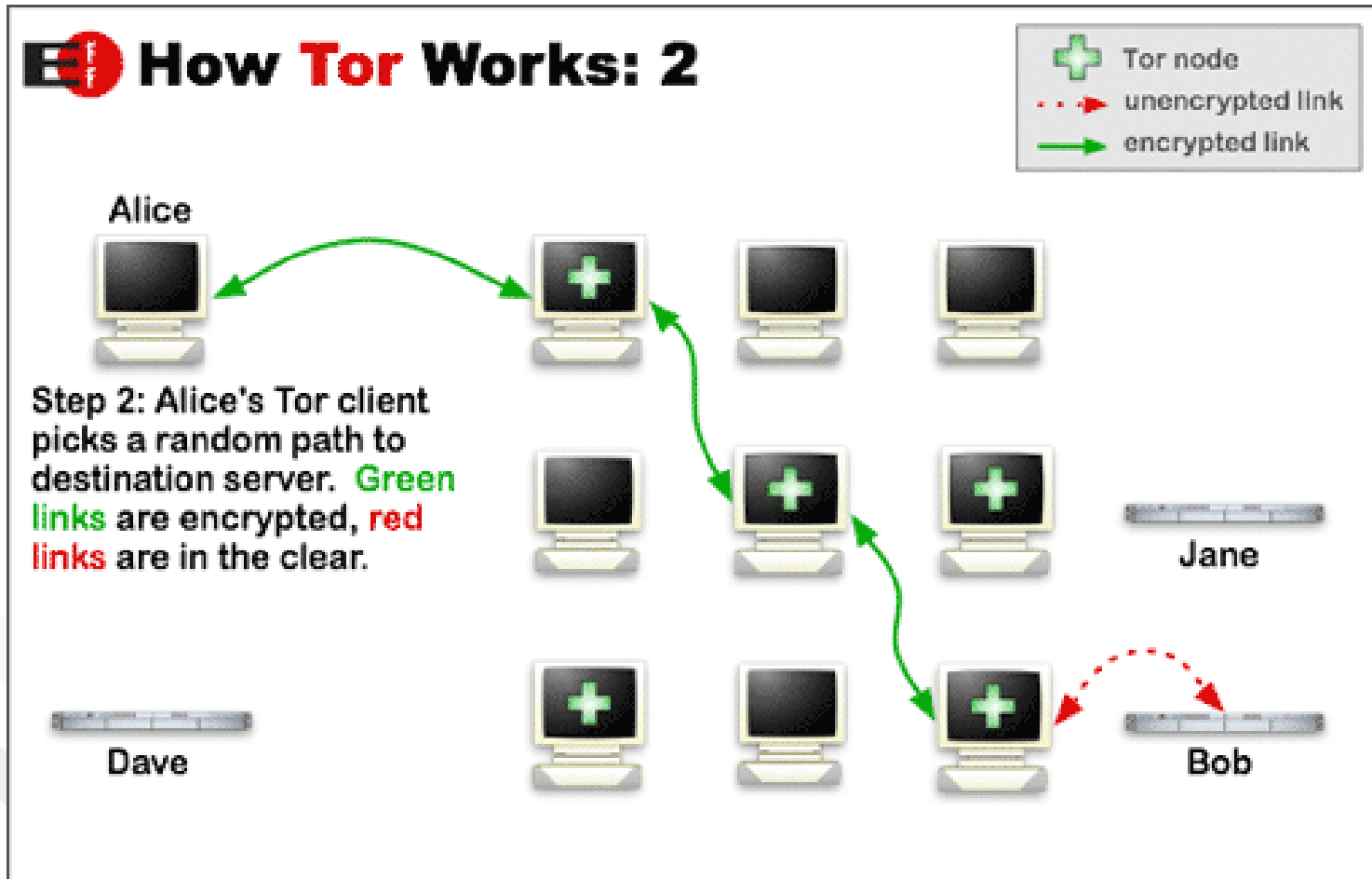
[Europe2006]

How Tor Works: 1

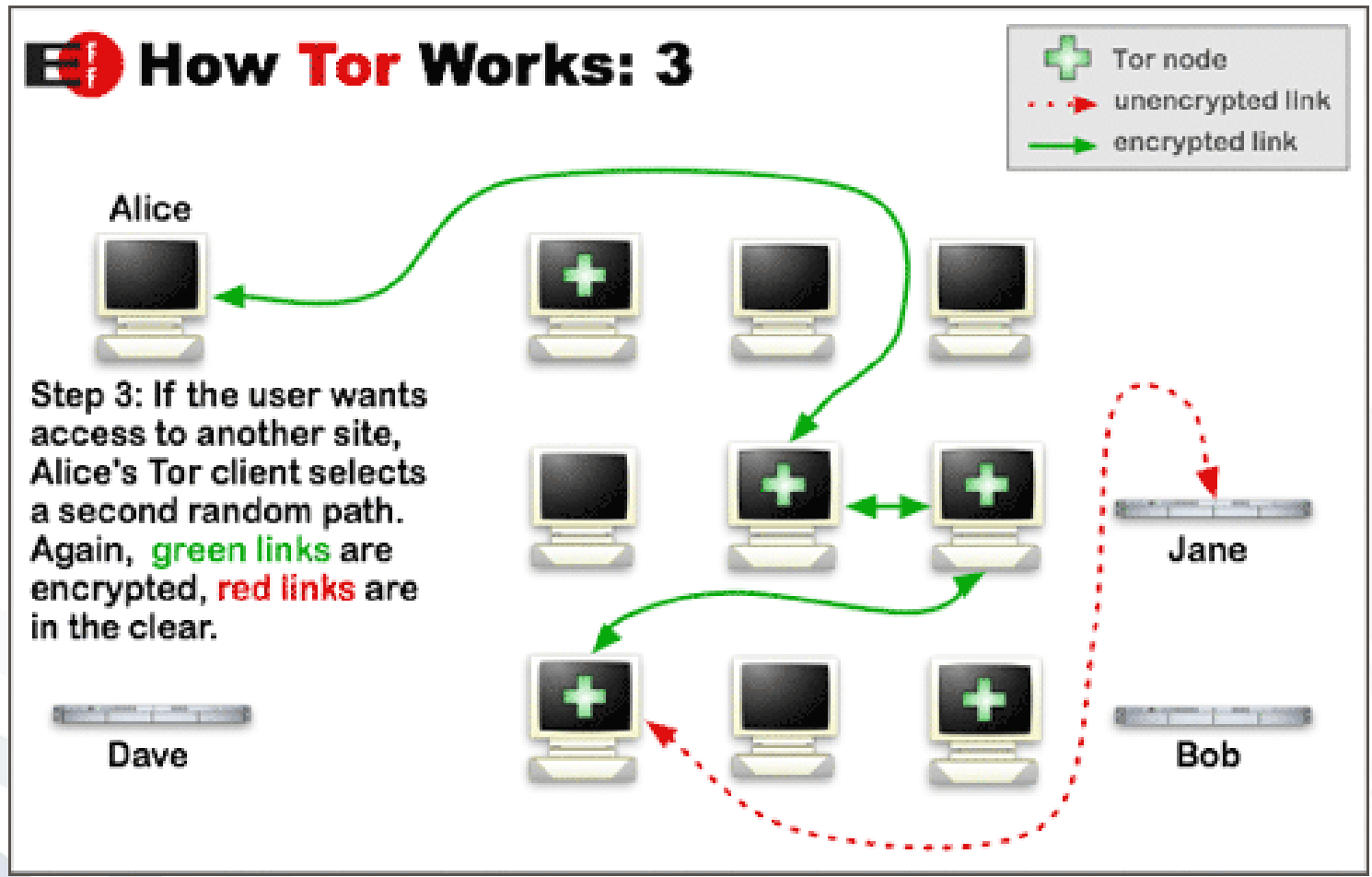
-  Tor node
-  unencrypted link
-  encrypted link



<http://tor.eff.org>



<http://tor.eff.org>

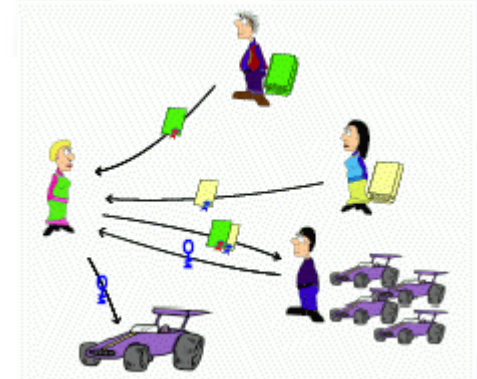


<http://tor.eff.org>

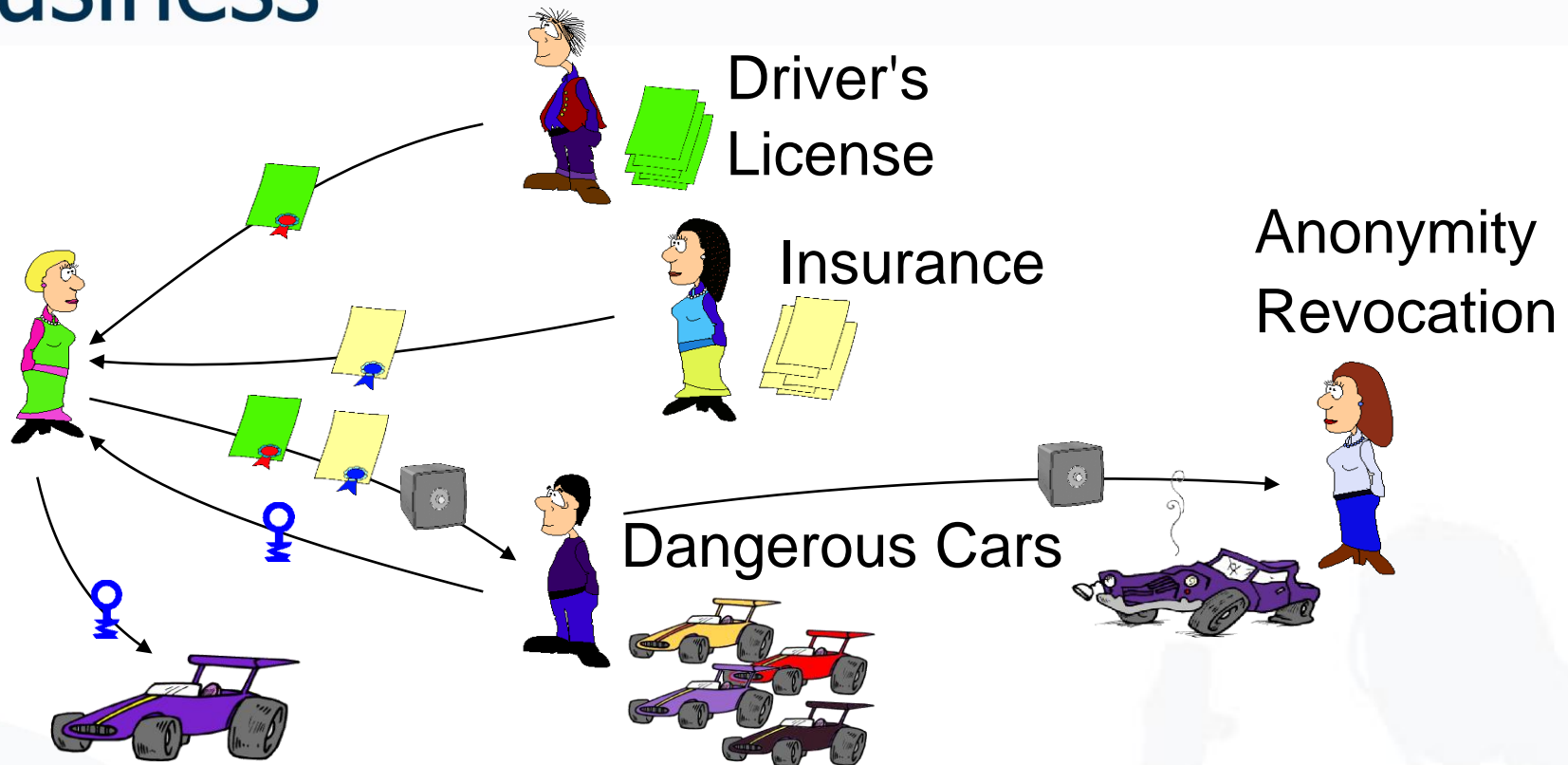
- Confuse data collectors
 - Exchange of cookies between users
 - Exchange of identities
 - Use of „faked“ data
- User-defined identity management
 - Assistance for the registration
 - Application of „real“ and „faked“ data
- Spam protection through disposable email addresses
- Ad blocking
- Integrated with JAP Anonymizer



- Anonymous Credentials are used to prove privileges or attributes of their owner without revealing its identity, e.g. to prove, that
 - a device contains an unrevoked Trusted Platform Module (TPM); this is also called Direct Anonymous Attestation
 - the owner possesses a subscription and is of the required age, e.g. for an identity management system supporting anonymous video download
- Such a system needs to have the following properties:
 - Unforgeability of credentials
 - Unlinkability of credentials
 - No credential sharing
 - Consistency of credentials



Idemix: Car Example



- What happens if a user exchanges information with multiple parties?
- The user has different pseudonyms with different parties.
- The user uses credentials to prove that he has a driver's license and an insurance.

- Standard of declaring privacy preferences in a standardized way
 - Snapshot of how a web site handles personal information about its users
 - P3P enabled browsers can "read" this snapshot and compare it to the consumer's set of privacy preferences.

- P3P enhances user control by
 - putting privacy policies where users can find them,
 - in a form users can understand, and
 - enables users to act on what they see.

- Unfortunately this promise has not yet been fulfilled.

Source: W3C P3P

DoNotTrack Flag



- Browsers are signaling advertising networks via the DoNotTrack Flag not to track the online behaviour of their users
- Problem: Advertising networks can either respect OR ignore the DoNotTrack Flag

Tracking Protection Lists



- Tracking Protection is build into the browser. Based on black lists, browsers prevent tracking data being transfer to advertising networks.
- Problems
 - Who maintains and updates the lists?
 - Do user understand the black list concept?
 - What if tracking protection is turned on by default?

PETs alone are not sufficient

- Anonymization and Pseudonymization
 - Mix-Master, Onion Routing, Anonymous Payment, Anonymous Credentials
 - A myriad of techniques and algorithms
- Playing Cat and Mouse with Big Brother
 - Best example is Cookie Cooker
 - But many people do not have the time.
- Good pragmatic tool, but still no success
 - ⇒ Integrated privacy protection,
 - ⇒ Into business processes
 - ⇒ Into user interfaces

- What is Privacy?
- Data Protection Directives and Laws
- Technical Data Protection
- General Requirements for Privacy
- Privacy by Design

General Privacy Requirements

- **Anonymity**
is the condition of not being identifiable within a set of subjects. The anonymity set for a given action is the set of all subjects who might have triggered the action.
- **Pseudonymity**
is an identifier used in place of the “real” identities, e.g., name, unique id number, of a given user. Pseudonymous identifiers can be made conditional and accountable using cryptographic building blocks.
- **Unlinkability**
is the condition in which a third party cannot determine whether two actions or two data items belong to a single user. Unlinkability is central to another privacy related concept called the separation of identities.

Source: GINI (2011)

- **Separation of Identities**
the condition of guaranteeing that separate partial identities of a given user are unlinkable.
- **Separation of Audiences**
the condition in which a user can control the audience of the information s/he reveals. The flexibility of the access control models determine the type of separation of audiences that can be practiced by the user.

Source: GINI (2011)

- What is Privacy?
- Data Protection Directives and Laws
- Technical Data Protection
- General Requirements for Privacy
- Privacy by Design

- Privacy by Design advances the view that the future of privacy cannot be assured solely by compliance with regulatory frameworks; rather, privacy assurance must ideally become an organization's default mode of operation.
- Privacy by Design states that privacy and data protection are embedded throughout the entire life cycle of technologies, from the early design stage to their deployment, use and ultimate disposal.
- The objectives of Privacy by Design – ensuring privacy and gaining personal control over one's information and, for organizations, gaining a sustainable competitive advantage – may be accomplished by practicing the 7 Foundational Principles

Source: Ann Cavoukian, Privacy Data Commissioner of Canada

Privacy by Design Principles

1. Proactive not Reactive; Preventative not Remedial
2. Privacy as the Default Setting
3. Privacy Embedded into Design
4. Full Functionality – Positive-Sum, not Zero-Sum
5. End-to-End Security – Full Lifecycle Protection
6. Visibility and Transparency – Keep it Open
7. Respect for User Privacy – Keep it User-Centric



- Bell, Tom W.: Internet Privacy and Self-Regulation: Lessons from the Porn Wars, Cato Institute Briefing Papers, No 65., 2001, www.cato.org/pubs/briefs/bp65.pdf
- Blarkom, G. W., Borking, John J., and Olk., J.G.: Handbook of Privacy and Privacy-Enhancing Technologies - PISA Privacy Incorporating Software Agent. The Hague, 2003.
- David Chaum: *Untraceable Electronic Mail, Return addresses, and Digital Pseudonyms*; Communications of the ACM February 1981 Volume 24 Number 2
- Hoofnagle, Chris Jay: Privacy Self Regulation: A Decade of Disappointment, 2005, www.epic.org/reports/decadedisappoint.html
- Reagle Jr, Joseph M., Boxed In: Why US Privacy Self Regulation Has Not Worked, Berkman Center for Internet & Society, Harvard Law School, 1998, <http://cyber.law.harvard.edu/people/reagle/privacy-selfreg.html>
- Self-Regulation: Regulatory Fad or Market Forces? Paper prepared for Cato Roundtable „Privacy vs, Innovation“ by Solveig Singleton, May 7, 1999, www.cato.org/pubs/wtpapers/990507report.html
- Varian Hal, Economic Aspects of Personal Privacy, Berkley University, 1996.
- Warren and Brandeis, The Right to Privacy”, Harvard Law Review., Vol. IV, December 15, 1890, No. 5

