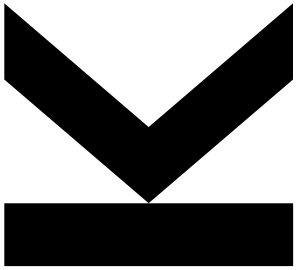
ANONYM IM INTERNET MITTELS TOR



Univ.-Prof. Dr. René Mayrhofer
4.12.2015: Schutz der Privatsphäre im Internet

JOHANNES KEPLER
UNIVERSITÄT LINZ

INSTITUTE
OF NETWORKS
AND SECURITY

PRIVATSPHÄRE ALS GRUNDRECHT

- **EU-Grundrechtecharta**
  - Recht auf Achtung des Privatlebens (Art. 7)
    Jede Person hat das Recht auf Achtung ihres Privat- und Familienlebens, ihrer Wohnung sowie ihrer Kommunikation.
  - Recht auf Schutz personenbezogener Daten (Art. 8)
    (1) Jede Person hat das Recht auf Schutz der sie betreffenden personenbezogenen Daten.
    (2) Diese Daten dürfen nur nach Treu und Glauben für festgelegte Zwecke und mit Einwilligung der betroffenen Person oder auf einer sonstigen gesetzlich geregelten legitimen Grundlage verarbeitet werden. Jede Person hat das Recht, Auskunft über die sie betreffenden erhobenen Daten zu erhalten und die Berichtigung der Daten zu erwirken.

Quelle: http://www.europarl.europa.eu/charter/pdf/text_de.pdf

PRIVATSPHÄRE ALS GRUNDRECHT

- **United Nations Human Rights**
  - “Universal Declaration of Human Rights” Article 12
  - “International Covenant on Civil and Political Rights” Article 17

  No one shall be subjected to arbitrary or unlawful interference with his privacy, family, home or correspondence, nor to unlawful attacks on his honour and reputation. Everyone has the right to the protection of the law against such interference or attacks.

Quelle: http://www.ohchr.org/en/udhr/pages/introduction.aspx, http://www.ohchr.org/EN/ProfessionalInterest/Pages/CCPR.aspx

PRIVATSPHÄRE ALS GRUNDRECHT

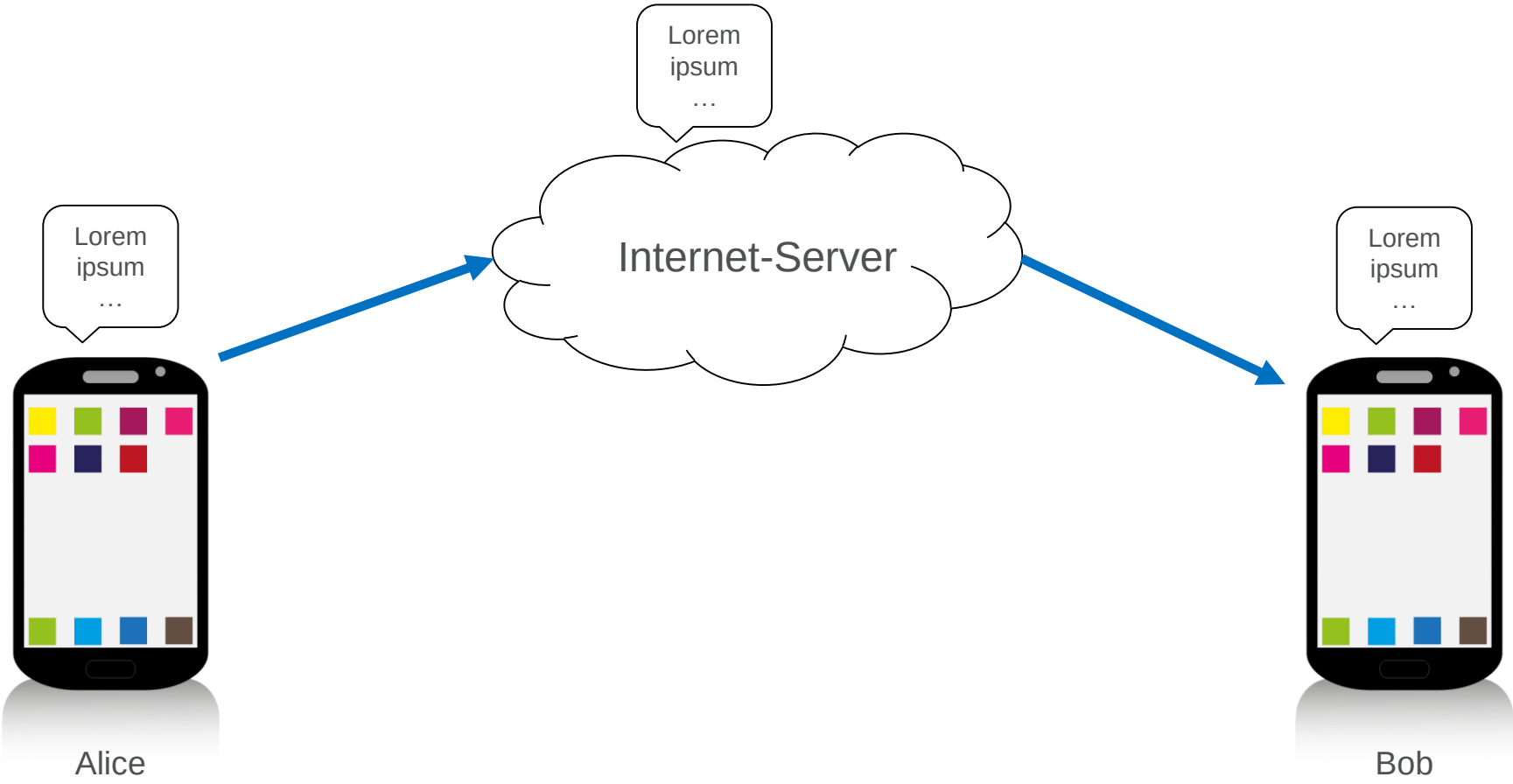
- **US „Bill of Rights“**: The Right to Privacy
  - Basiert auf Artikel von Samuel D. Warren und Louis Brandeis aus dem Jahr 1890
  - Formuliert als "**right to be let alone**"

Mehr Details: https://en.necessaryandproportionate.org/text

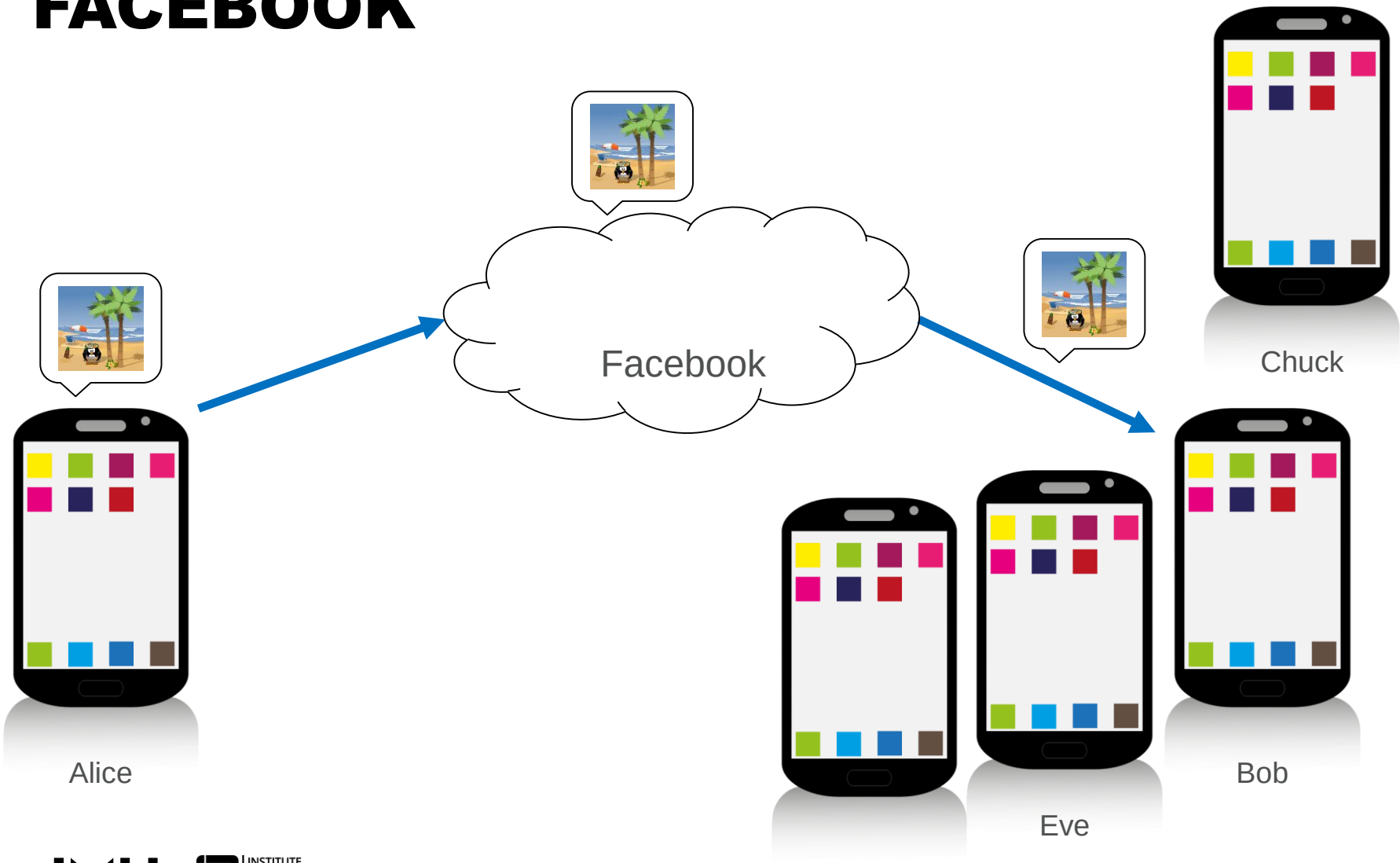
ALLTÄGLICHES TRACKING IM INTERNET

- Überwachung von Kommunikation im Internet durch
  - Unternehmen und Service-Provider
  - Kriminelle Organisationen
  - Staatliche Geheimdienste
- Aufzeichnung unzähliger Datenpunkte
  - Quelle und Ziel der Kommunikation
    - bei Emails: Sender und Empfänger
    - beim Websurfen: Client und abgefragte Seiten
  - Zeitpunkt und Menge der übertragenen Daten
  - Physischer Ort von Quelle und Ziel
  - Manchmal auch alle Inhalte
- Schwer nachzuvollziehen, wer wann welche Daten über wen aufzeichnet und wie lange diese gespeichert bleiben

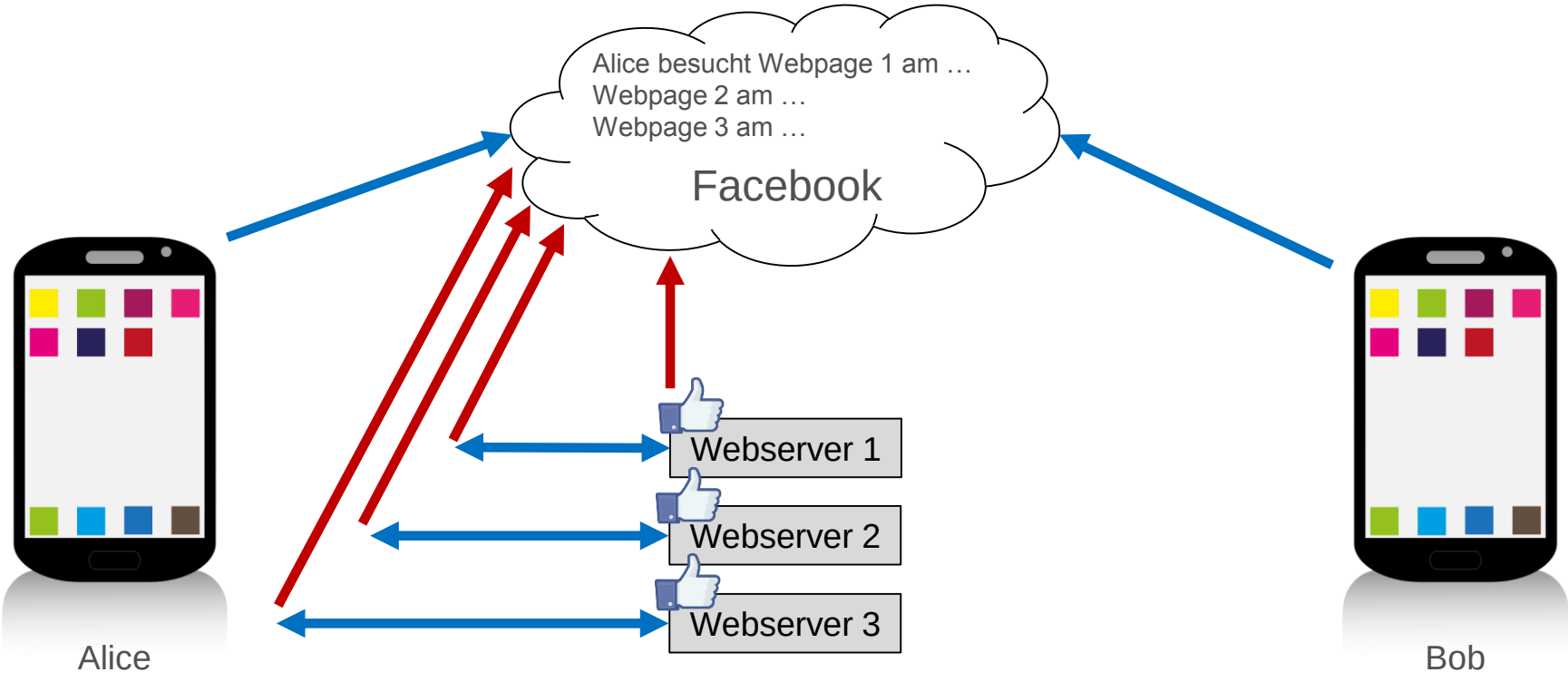
TRACKING AM BEISPIEL INSTANT MESSAGING



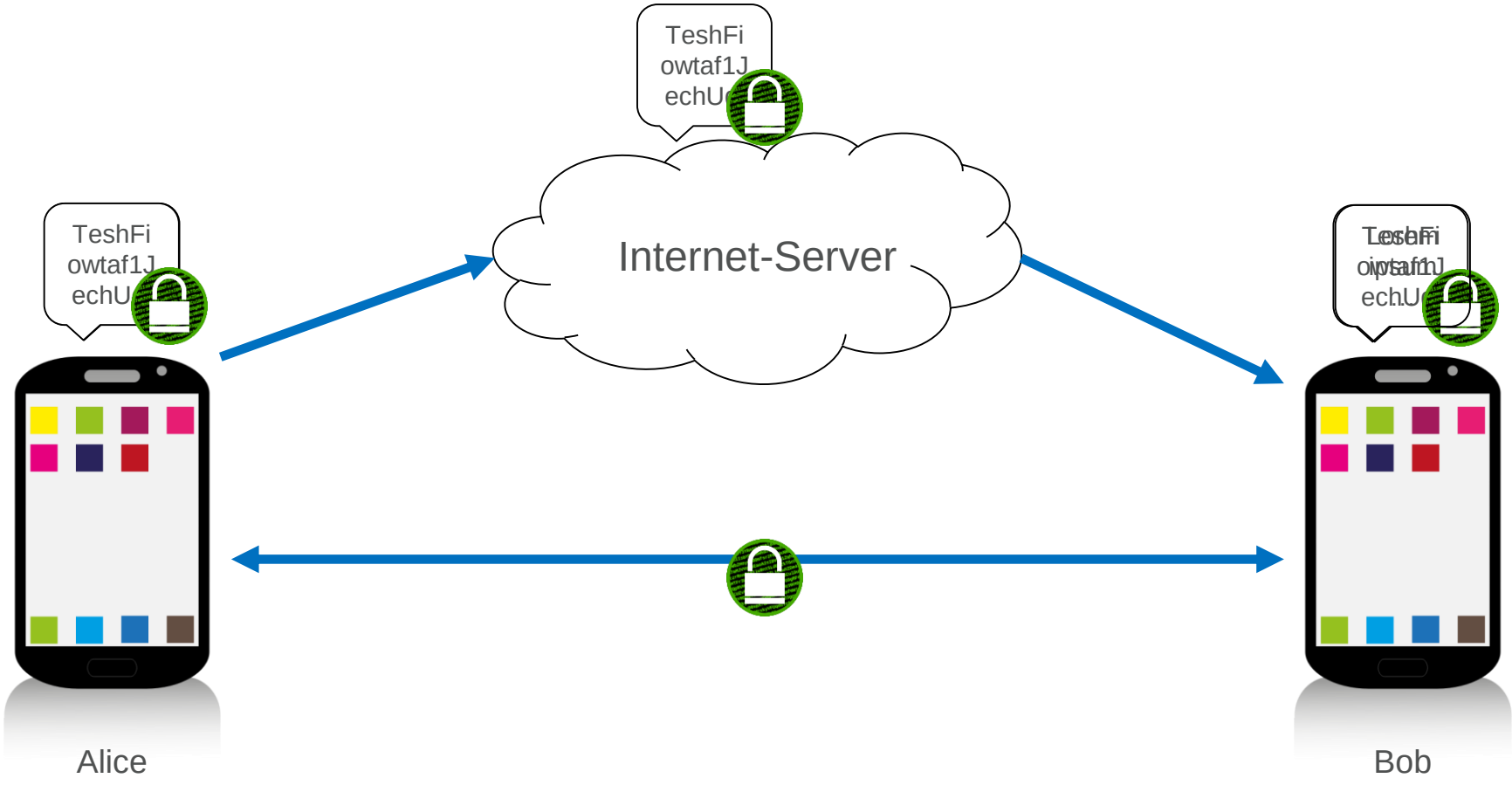
TRACKING AM BEISPIEL FACEBOOK



TRACKING AM BEISPIEL FACEBOOK



TRACKING AM BEISPIEL TELEFONIE/TEXT MIT „SIGNAL“



MÖGLICHKEITEN FÜR ANONYMITÄT IM INTERNET

- Öffentliche Internet-Terminals
  - Bibliotheken, Universitäten, …
  - Flughäfen, Bahnhöfe, …
  - Internet-Cafes
- Offene WLAN Hotspots
  - Stadt Linz und viele andere Städte weltweit
  - Öffentlicher Verkehr
  - Hotels, Restaurants, Einkaufszentren
- Prepaid SIM-Karten
  - In Österreich und anderen Ländern ohne Identifizierung
- Andere VPN- und Proxy-Dienste im Internet (z.T. kostenpflichtig)

PROBLEM DIESER METHODEN

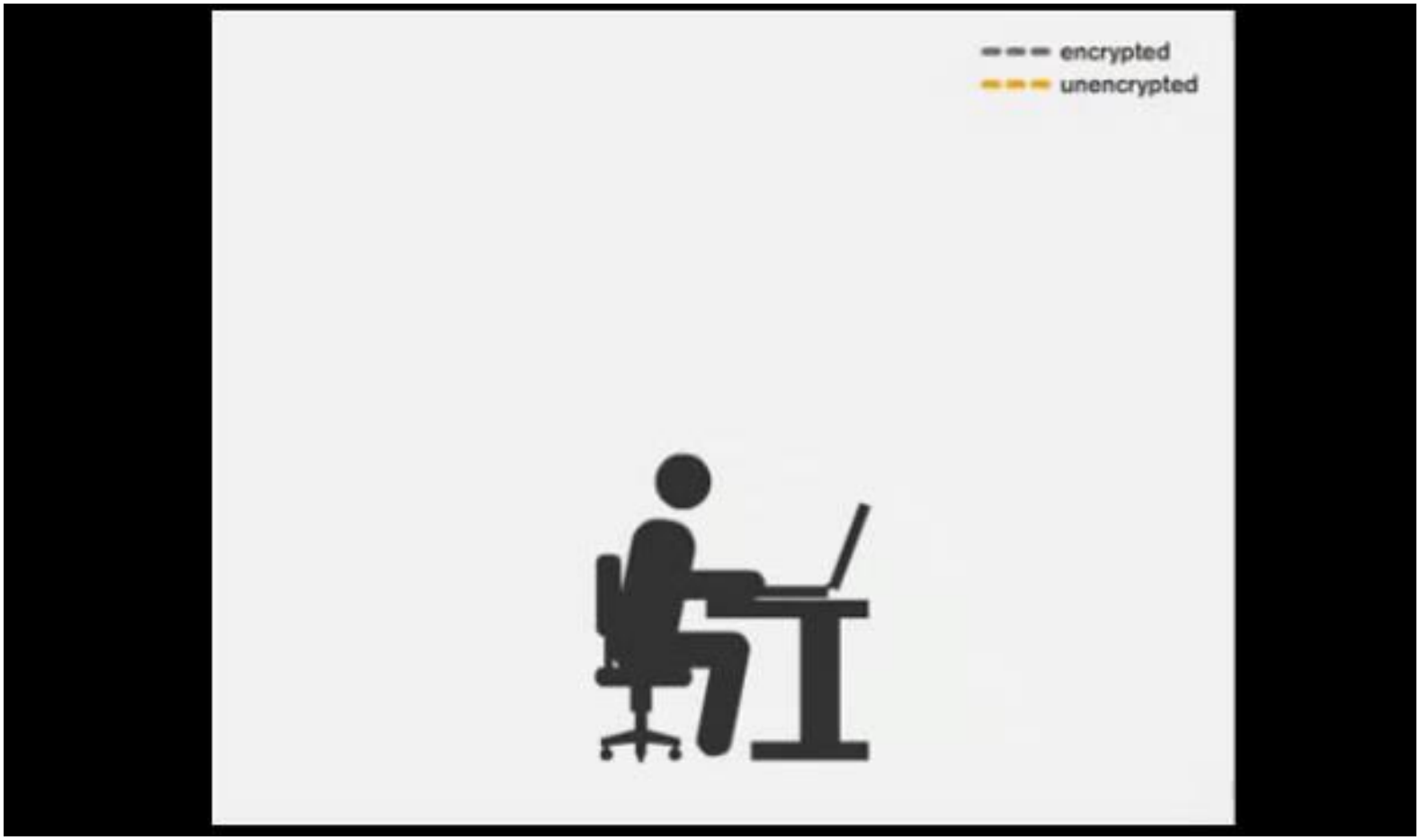
- **Unbequem !**
  - Nicht vom eigenen Endgerät (Laptop, Smartphone, …) aus
  - Nicht vom eigenen Internet-Anschluss aus
  - Nicht von der eigenen Wohnung aus
  - Nicht mit den eigenen Daten am Gerät
- Folge: Bequemlichkeit siegt → auf Anonymität wird verzichtet
- Für praktikable Anonymität sollte diese
  - an jedem Internetanschluss
  - mit (fast) jedem Endgerät
  - zu jeder Zeit
  - für alle Benutzer

  verfügbar sein

TOR: THE ONION ROUTER

- Open Source Projekt zur Anonymisierung im Internet
- Basiert auf Prinzip des **Onion Routing**
  - Ursprünglich entwickelt von US Naval Research Laboratory
  - Vermittelt Internetverbindungen über drei Relays
    - Entry Node
    - Middle Node
    - Exit Node
  - Erste Version wurde 2004 öffentlich verfügbar gemacht
- Wird aktiv weiterentwickelt
  - „The Tor Project“ als Organisation zur Weiterentwicklung
  - Ab 2006 unterstützt durch Electronic Frontier Foundation (EFF)

TOR: THE ONION ROUTER



Quelle: http://video.mit.edu/watch/how-tor-works-502/

LIVE-DEMO

- http://mybrowserinfo.net/detail.asp
- http://iplocation.net
- http://beta.speedtest.net

AUSWIRKUNGEN VON TOR AUF CLIENTS

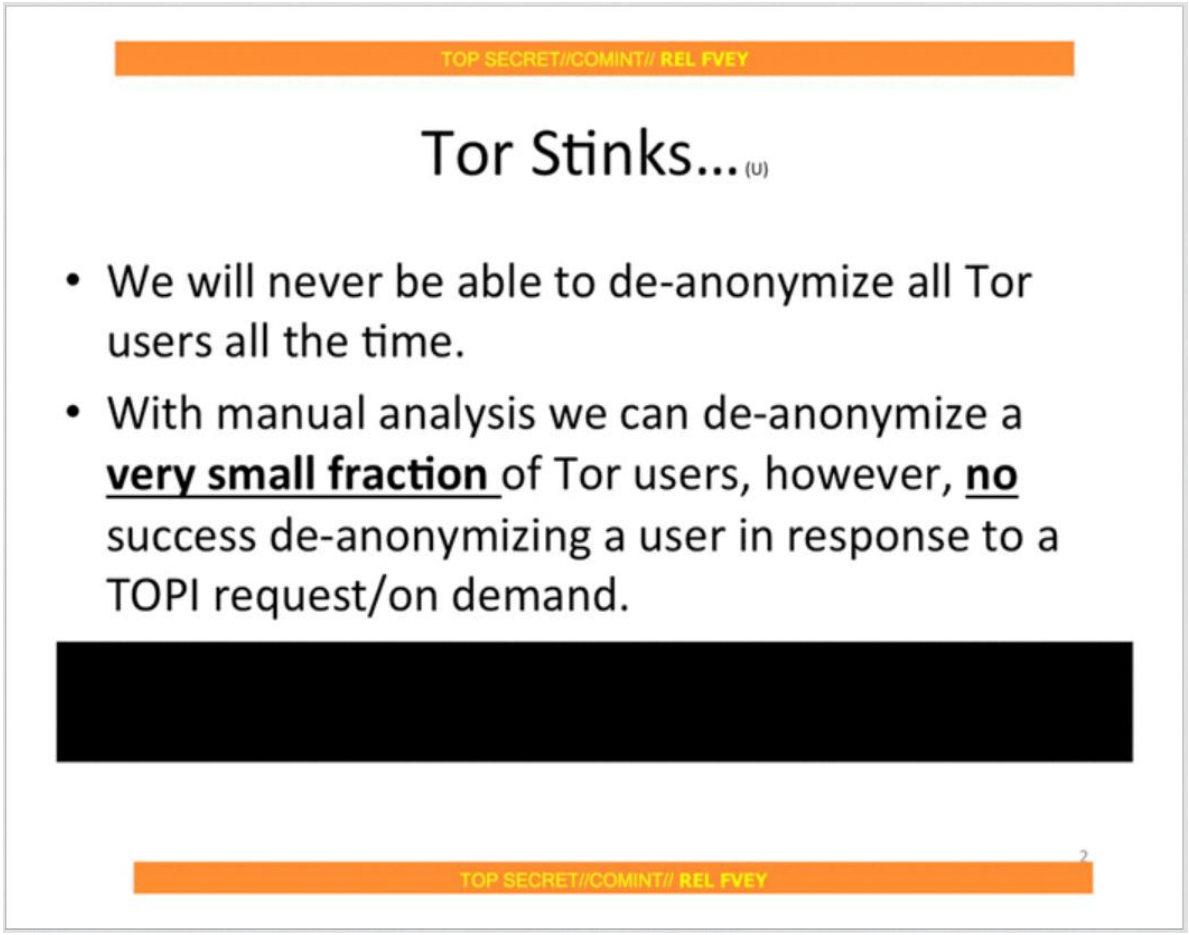
- Performance der Verbindungen sinkt
  - Bandbreite wird geringer – abhängig von der eigenen Internet-Anbindung und den gewählten Relays
  - Latenz (Übertragungsverzögerung) steigt signifikant
- Manche Zielserver schränken Verbindungen von Tor ein
  - z.B. Google: manchmal Abfrage nach CAPTCHA
  - Wenige Webserver blockieren Verbindungen ganz
- Manchmal angenehme Funktionen funktionieren nicht mehr
  - z.B. Auswahl der nächstgelegenen Standorte
  - z.B. Auswahl der Sprache

  wenn basierend auf der Quell-IP-Adresse

TOR HIDDEN SERVICES

- Zusätzlich zum „Tunneling“ von herkömmlichen TCP und UDP Verbindungen von Clients zu Servern
- Server können neue Identität erzeugen und diese im Tor-Netzwerk bei zufällig ausgewählten Relays registrieren
- Statt typischen Hostnamen (www.abc.com) wird eine Pseudo-Domain mit kryptographisch generierten Namen (abgeleitet von der Identität des Servers) verwendet
  - z.B. SecureDrop für „The Intercept“: y6xjgkgwj47us5ca.onion
- IP-Adresse des **Servers** bleibt für Client und die meisten Relays verborgen
  - Gegensatz zu „normalem“ Einsatz von Tor: Client-Adressen anonymisiert, Server aber mit öffentlich bekannter Adresse

AUSWIRKUNGEN VON TOR AUF ÜBERWACHUNGSMAßNAHMEN

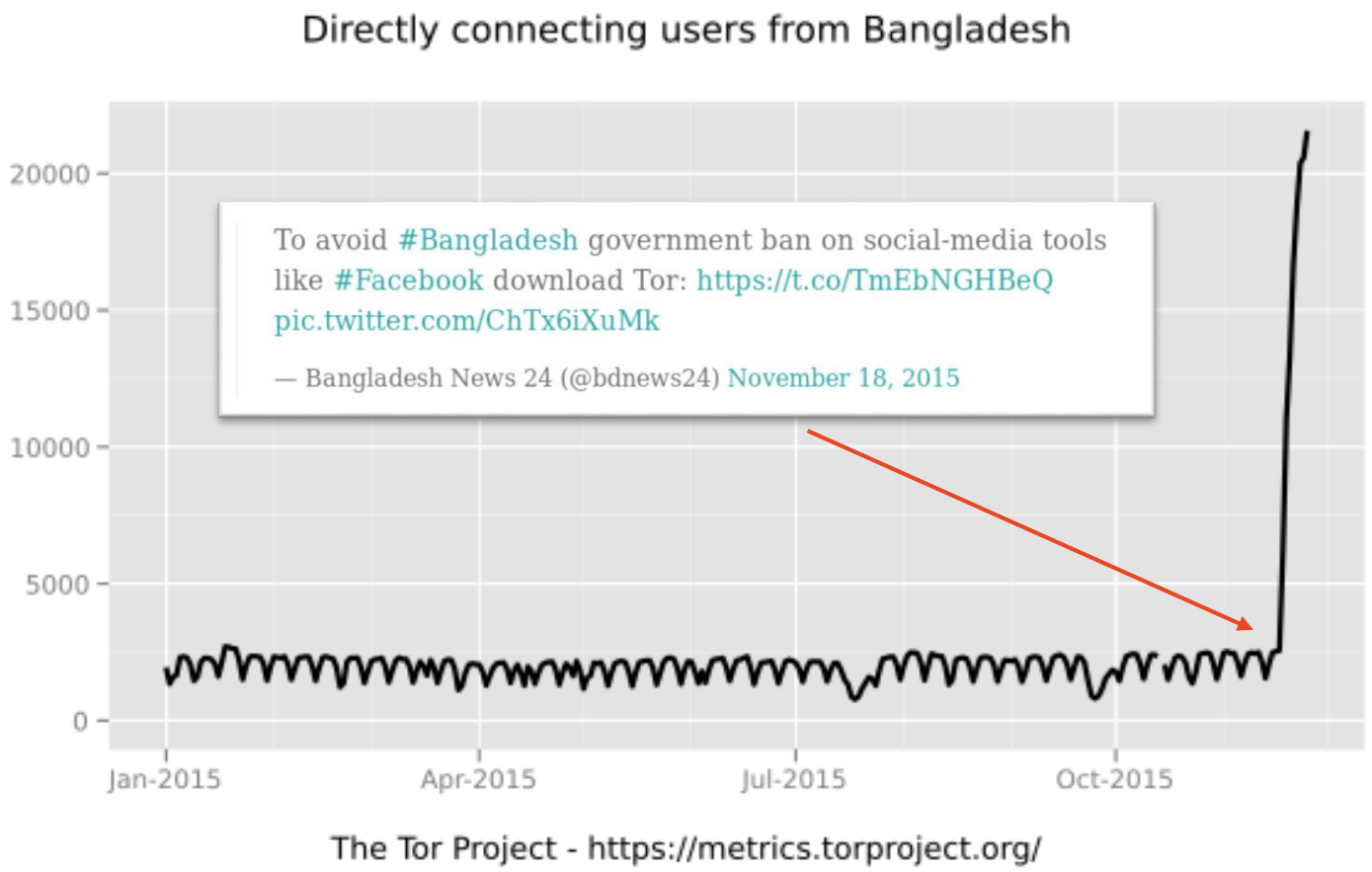


Quelle: http://www.theguardian.com/world/interactive/2013/oct/04/tor-stinks-nsa-presentation-document

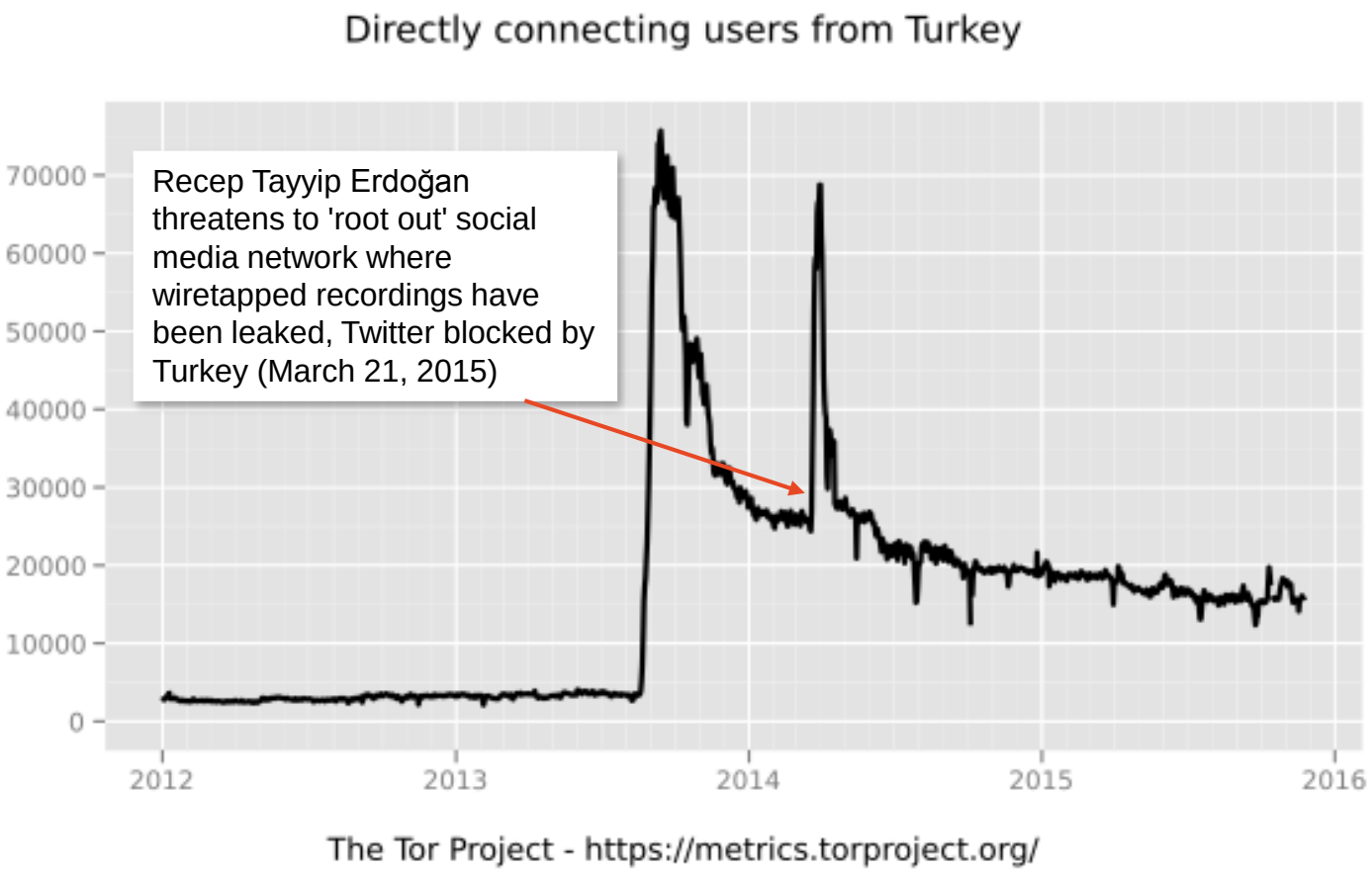
WER VERWENDET TOR?

- Bürger in restriktiven Staaten
  - Westliche Journalisten in Kommunikation mit Whistle Blowern
  - Edward Snowden als bekanntester Benutzer

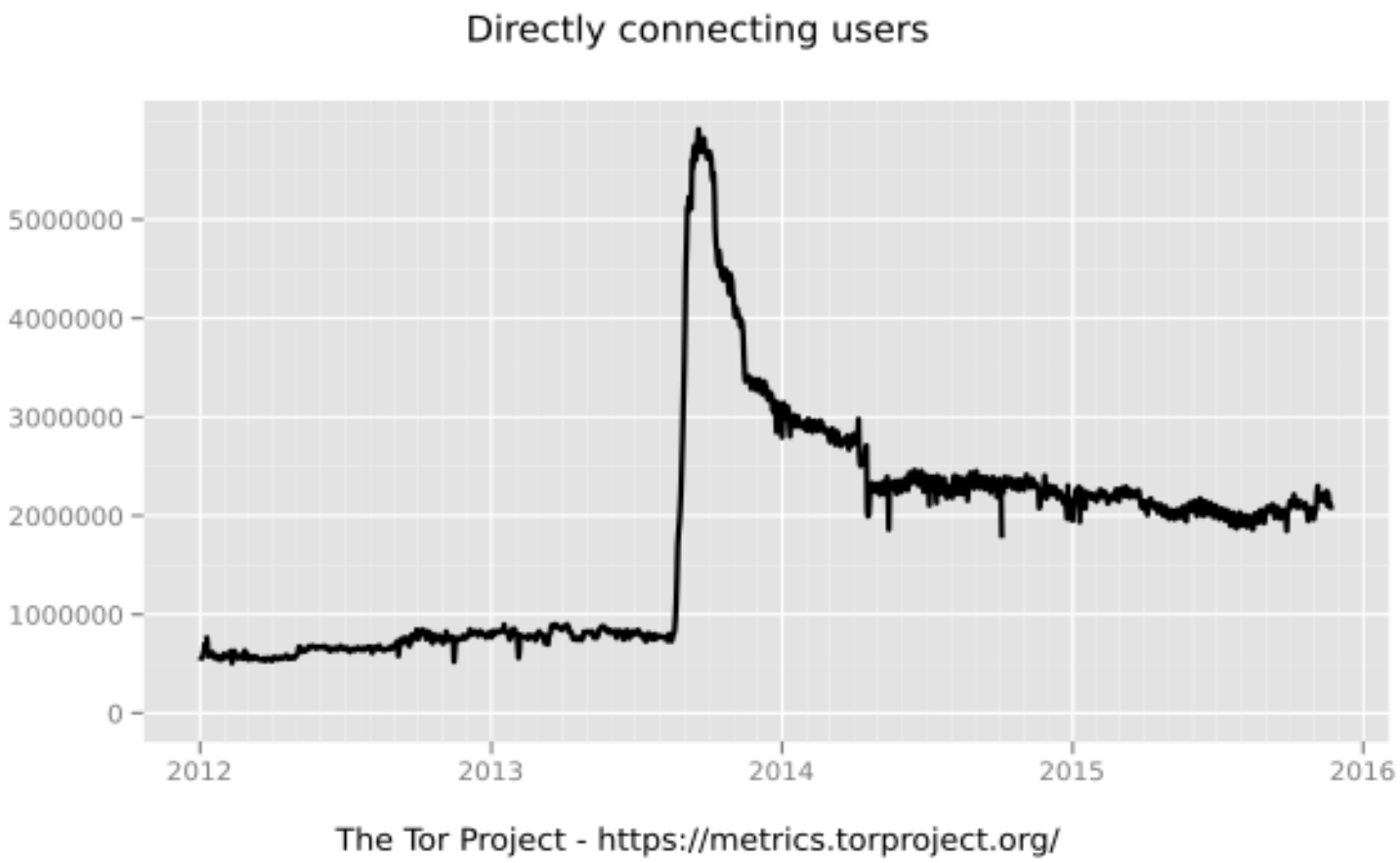
WER VERWENDET TOR?



WER VERWENDET TOR?



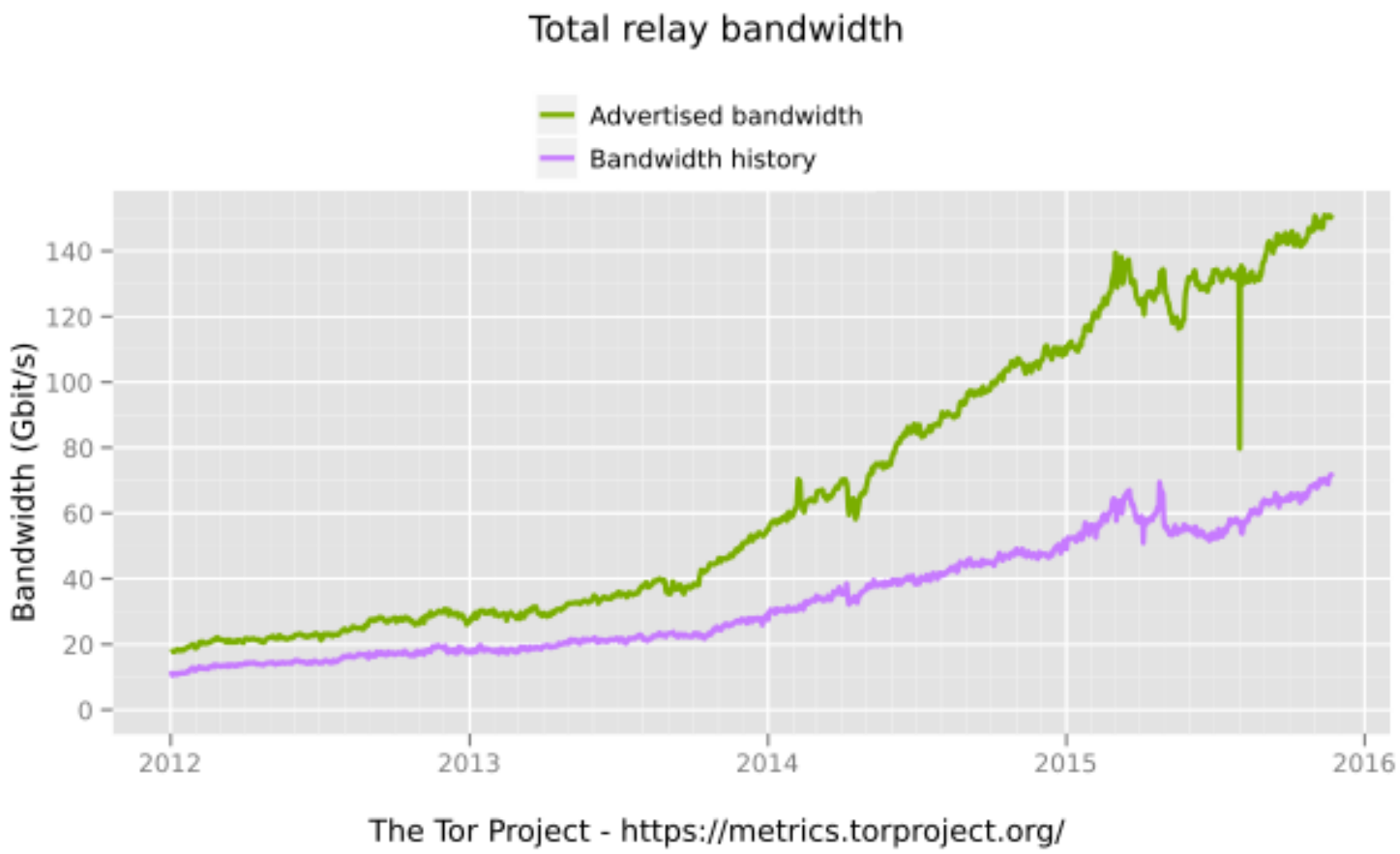
WER VERWENDET TOR?



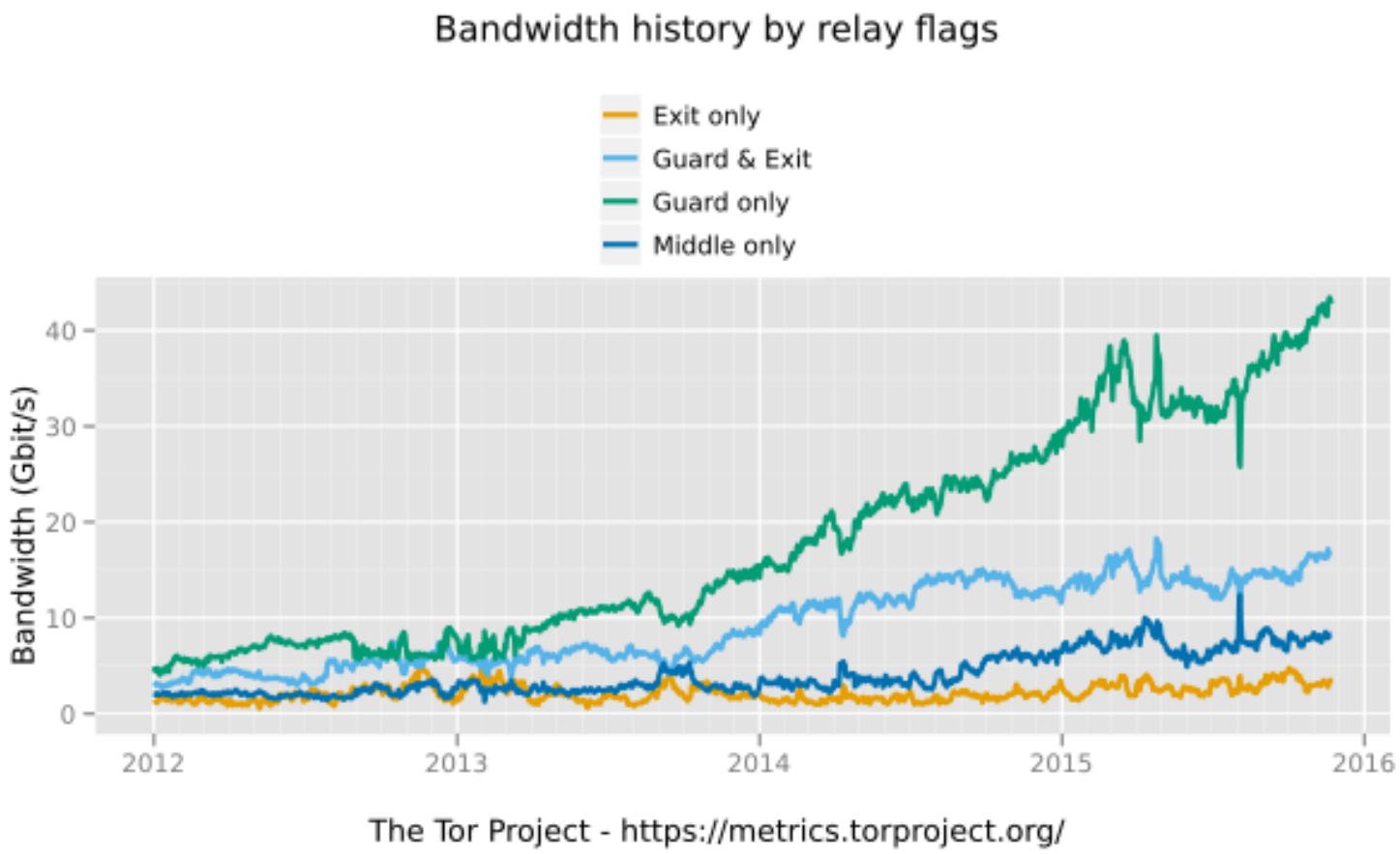
WER VERWENDET TOR?

- Bürger in Bangladesch, Türkei, Chinesische Journalisten, Blogger, etc.
  - Westliche Journalisten in Kommunikation mit Whistle Blowern
  - Edward Snowden als bekanntester Benutzer
- Unternehmen zur Verhinderung von Wirtschaftsspionage
- Kriminelle
  - Verschleierung der Kommunikation (z.B. Wiederbetätigung)
  - Schadsoftware zum Verstecken der Command&Control-Server
- Und ich, seit knapp 10 Jahren ☺
  - nicht als Abwehr von staatlicher Überwachung, sondern gegen Tracking durch Facebook, Google, Ad-Netzwerke, …
  - seit ca. 12 Monaten deutlich praktikabler weil steigende Performance im Tor-Netzwerk

WER VERWENDET TOR? GESAMTE RELAY-BANDBREITE



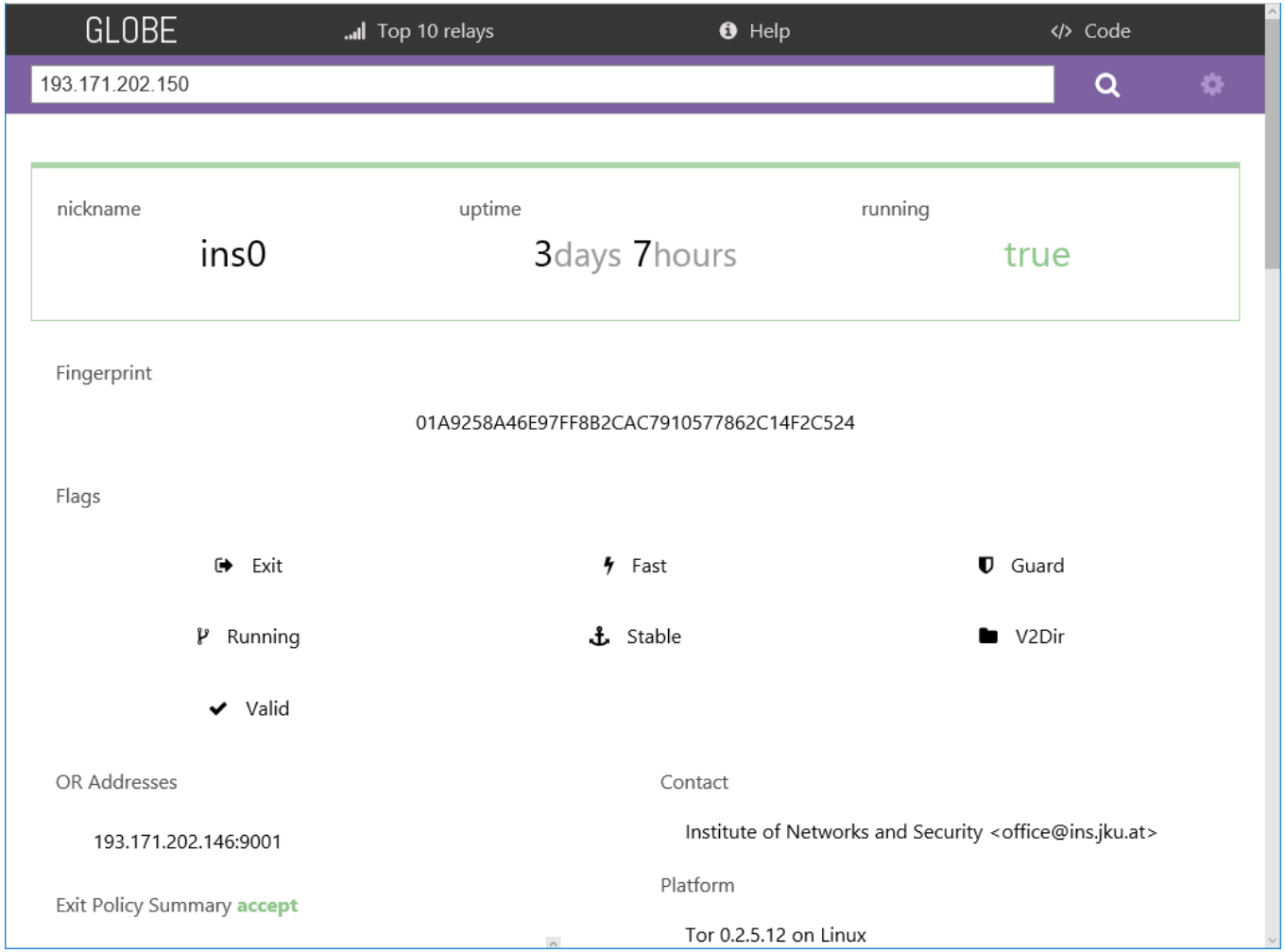
WER VERWENDET TOR? BANDBREITE PRO NODE-TYP



DER TOR EXIT NODE AN DER JKU ALS FORSCHUNGSPROJEKT

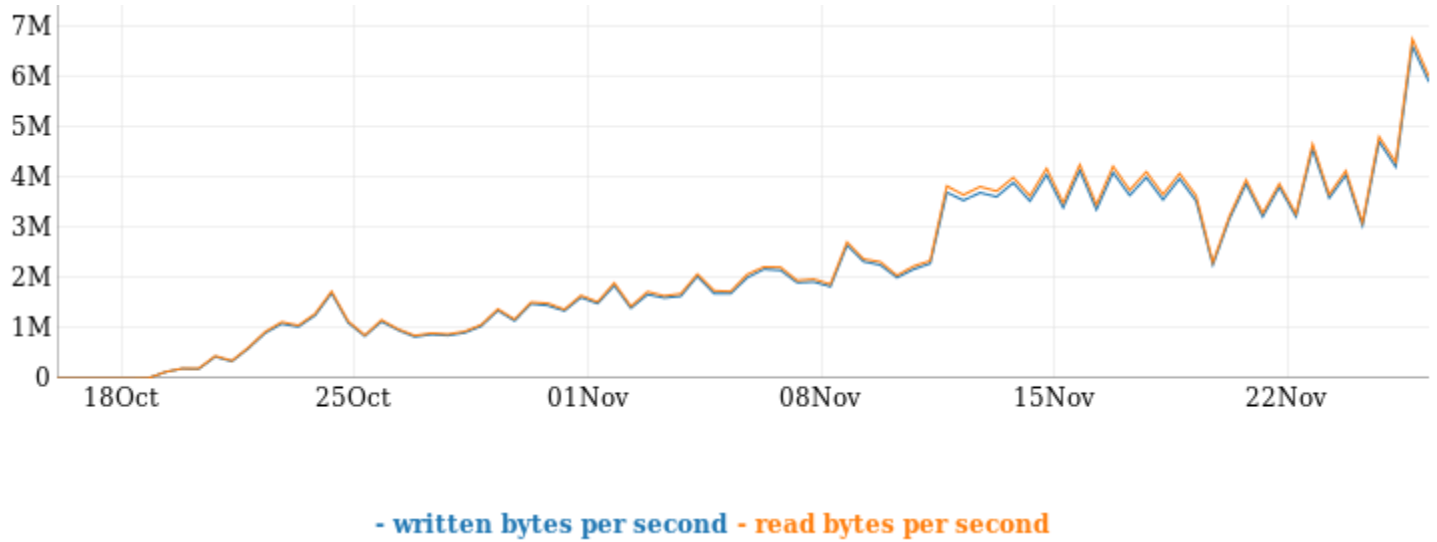
- Warum?
  - Neutrale, ergebnisoffene Forschung
  - Interessante Schnittstelle zwischen Technik und Recht
  - Interessante Probleme für Netzwerkkommunikation
  - Interessante Probleme in der Balance zwischen notwendiger Strafverfolgung von Kriminellen und essentieller Privatsphäre der allgemeinen Bevölkerung
  - Aufbau von objektiver Kompetenz für Datenschutzbeauftragte, Strafverfolgungsbehörden, Bürgerrechtsorganisationen, Lehre
- Wie? → Dr. Rudolf Hörmannseder
- Was? → Assoc.-Prof. Dr. Michael Sonntag

AKTUELLE DATEN ZUM JKU EXIT



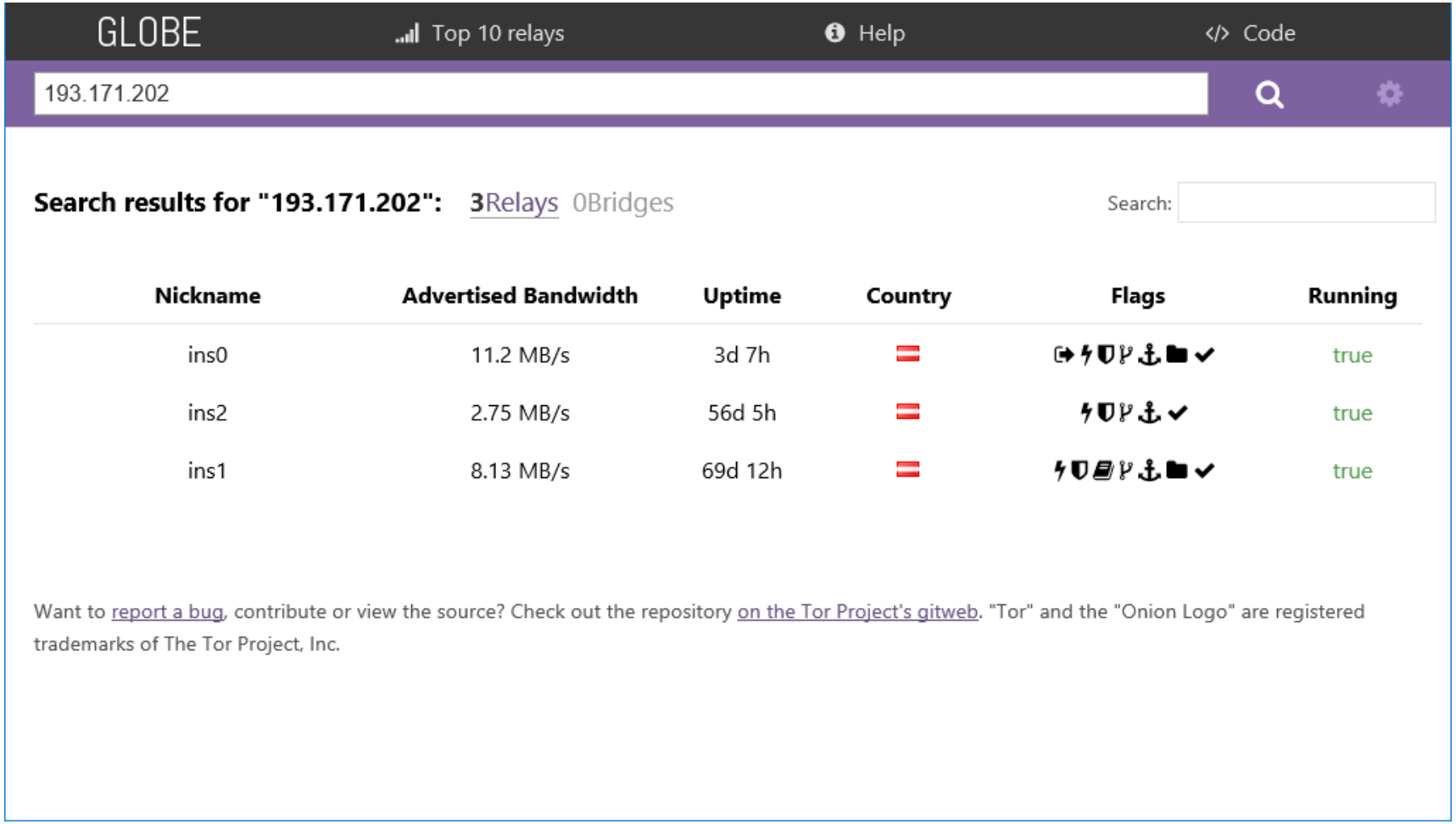
Aktuelle Daten: https://globe.torproject.org/#/search/query=193.171.202.150

AKTUELLE DATEN ZUM JKU EXIT



Aktuelle Daten: https://globe.torproject.org/#/search/query=193.171.202.150

PRODUKTIV- UND TESTSERVER



Aktuelle Daten: https://globe.torproject.org/#/search/query=193.171.202

ANDERE INITIATIVEN RUND UM TOR IN DEN JAHREN 2014 UND 2015

- Library Freedom Project
  - Öffentliche Internet-Terminals mit Tor Clients
  - Exit Nodes
- Carnegie Mellon University
  - Unterstützung des FBI bei proaktiver Überwachung
  - Ausnutzung einer Sicherheitslücke in Tor
  - Konkrete Forschung ist derzeit ethisch umstritten
- SecureDrop
  - Zur Unterstützung von Whistle Blowern
  - Wird von Medienunternehmen eingesetzt, um sicheres und anonymes Einliefern von Information zu ermöglichen

Mehr Details: https://libraryfreedomproject.org/, https://blog.torproject.org/category/tags/cmu, https://securedrop.org/

JOHANNES KEPLER
UNIVERSITÄT LINZ

VIELEN DANK FÜR IHRE AUFMERKSAMKEIT!

https://ins.jku.at/research/projects/tor

JOHANNES KEPLER
UNIVERSITÄT LINZ
Altenberger Straße 69
4040 Linz, Österreich
www.jku.at