



Schutz vor Beobachtung im Internet

Prof. Dr. Hannes Federrath

Sicherheit in verteilten Systemen (SVS)

<http://svs.informatik.uni-hamburg.de>

Warum Datenschutz?

Geburtsdatum Telefonnummer

Name, Vorname Wohnort

Steuernummer Autokennzeichen

Kontonummer E-Mail-Adresse

Religionszugehörigkeit

Krankenversicherungs-Nr.

Kreditkarten-Nr.

Grundbuch- und
Katasterbezeichnung

Personenbezogene Daten sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden »betroffene Person«) beziehen. – Def. nach Art. 4 Nr. 1 DSGVO

CATEGORIES OF PERSONAL INFORMATION

The following are categories of information relating to an individual, whether it relates to his or her private, professional or public life. Categories are not exclusive. Information may transcend multiple categories.



INTERNAL



Knowledge and Belief

Information about what a person knows or believes religious beliefs, philosophical beliefs, thoughts, what they know and don't know, what someone thinks



Authenticating

Information used to authenticate an individual with something they know passwords, PIN, mother's maiden name



Preference

Information about an individual's preferences or interests opinions, intentions, interests, favorite foods, colors, likes, dislikes, music



EXTERNAL



Identifying

Information that uniquely or semi-uniquely identifies a specific individual name, user-name, unique identifier, government issued identification, picture, biometric data



Ethnicity

Information that describes an individual's origins and lineage race, national or ethnic origin, languages spoken, dialects, accents



Sexual

Information that describes an individual's sexual life gender identity, preferences, proclivities, fetishes, history, etc.



Behavioral

Information that describes an individual's behavior or activity, on-line or off browsing behavior, call logs, links clicked, demeanor, attitude



Demographic

Information that describes an individual's characteristics shared with others age ranges, physical traits, income brackets, geographic



Medical and Health

Information that describes an individual's health, medical conditions or health care physical and mental health, drug test results, disabilities, family or individual health history, health records, blood type, DNA code, prescriptions



Physical Characteristic

Information that describes an individual's physical characteristics height, weight, age, hair color, skin tone, tattoos, gender, piercings



HISTORICAL



Life History

Information about an individual's personal history events that happened in a person's life, either to them or just around them which might have influenced them (WWII, 9/11)

FINANCIAL



Account

Information that identifies an individual's financial account credit card number, bank account



Ownership

Information about things an individual has owned, rented, borrowed, possessed cars, houses, apartments, personal possessions



Transactional

Information about an individual's purchasing, spending or income purchases, sales, credit, income, loan records, transactions, taxes, purchases and spending habits



Credit

Information about an individual's reputation with regards to money credit records, credit worthiness, credit standing, credit capacity

SOCIAL



Professional

Information about an individual's educational or professional career job titles, salary, work history, school attended, employee files, employment history, evaluations, references, interviews, certifications, disciplinary actions



Criminal

Information about an individual's criminal activity convictions, charges, pardons

Public Life

Information about an individual's public life character, general reputation, social status, marital status, religion, political affiliations, interactions, communications meta-data



Family

Information about an individual's family and relationships family structure, siblings, offspring, marriages, divorces, relationships



Social Network

Information about an individual's friends or social connections friends, connections, acquaintances, associations, group membership

Communication

Information communicated from or to an individual telephone recordings, voice mail, email



TRACKING



Computer Device

Information about a device that an individual uses for personal use (even part-time or with others) IP address, Mac address, browser fingerprint



Contact

Information that provides a mechanism for contacting an individual email address, physical address, telephone number



Location

Information about an individual's location country, GPS coordinates, room number

Recht auf informationelle Selbstbestimmung

«Freie Entfaltung der Persönlichkeit setzt unter den modernen Bedingungen der Datenverarbeitung den *Schutz des Einzelnen gegen unbegrenzte Erhebung, Speicherung, Verwendung und Weitergabe seiner persönlichen Daten* voraus. ...

Wer nicht mit hinreichender Sicherheit überschauen kann, welche ihn betreffenden Informationen in bestimmten Bereichen seiner sozialen Umwelt bekannt sind, und wer das Wissen möglicher Kommunikationspartner nicht einigermaßen abzuschätzen vermag, kann in seiner Freiheit wesentlich gehemmt werden, aus eigener Selbstbestimmung zu planen oder zu entscheiden.

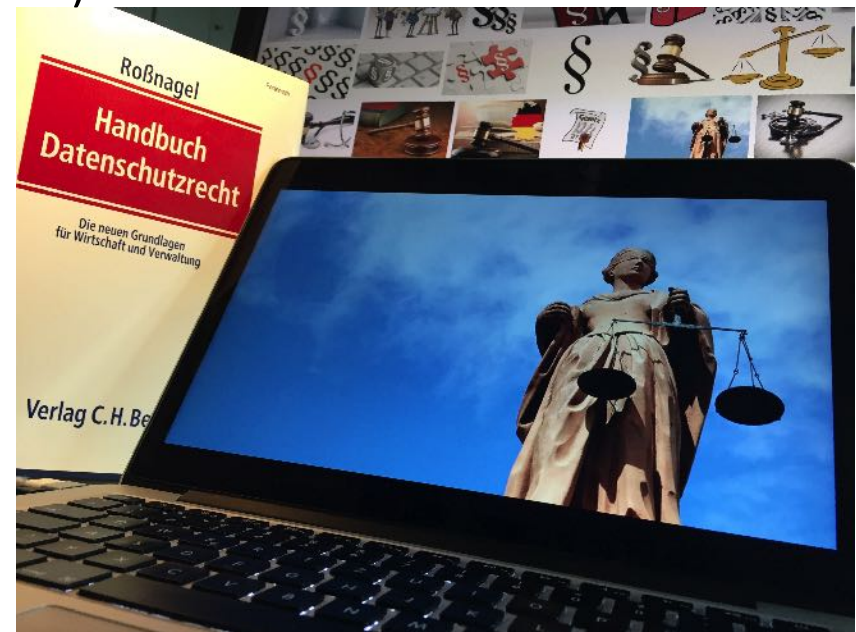
Mit dem Recht auf informationelle Selbstbestimmung wäre eine Gesellschaftsordnung nicht vereinbar, in der Bürger nicht mehr wissen können, wer was wann und bei welcher Gelegenheit über sie weiß.»

aus dem Volkszählungsurteil des Bundesverfassungsgerichts
vom 15. Dezember 1983 1 BvR 209/83 Abschnitt C II.1, S. 43

Recht auf informationelle Selbstbestimmung

Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben.

- **Datenschutz**
 - = Schutz der Menschen
 - ≠ (Schutz der Daten = Datensicherheit)
- Ab 2018 europaweit einheitlich geregelt über eine EU-Datenschutz-Grundverordnung



Recht auf informationelle Selbstbestimmung

Mit dem Begriff Datenschutz wird das Recht des Einzelnen auf informationelle Selbstbestimmung umschrieben.

- Recht auf informationelle Selbstbestimmung = Grundrecht
- Herleitung des Rechts auf informationelle Selbstbestimmung
 - aus dem Allgemeinen Persönlichkeitsrecht gemäß Art. 2 Abs. 1 i.V.m. Art. 1 Abs. 1 Grundgesetz (GG) durch das Bundesverfassungsgericht im Volkszählungsurteil
- «Volkszählungsurteil» des Bundesverfassungsgerichts vom 15.12.1983:
 - «Das Grundrecht gewährleistet [...] die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.»

Grundrechtsnormen als Abwehrrechte gegen den Staat

Grundrechtsnormen wurden als Abwehrrechte der Grundrechtsträger gegen den Staat konzipiert.

■ Frage:

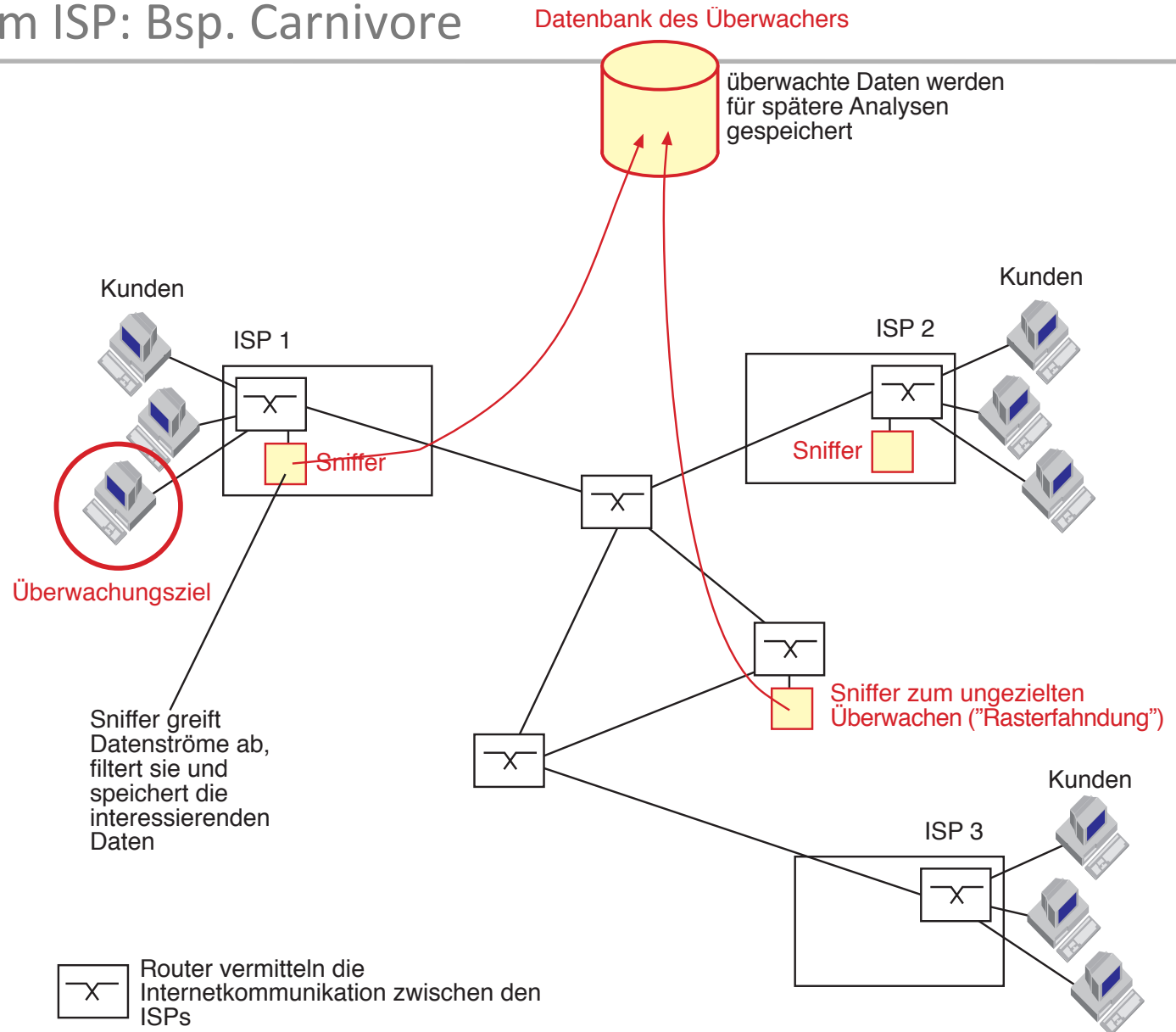
- Können Grundrechte auch in der Beziehung Privater untereinander bedeutsam und wirksam sein?

■ Dritt- oder Horizontalwirkung der Grundrechte

- Grundrechtsnormen sind auch «objektiv-rechtlich fundierte Aufträge an den Staat zur näheren Ausgestaltung der Möglichkeit des Freiheitsgebrauchs und zum Freiheitsschutz auch gegenüber Gefährdungen durch Private» (Hoffmann-Riem 2018, S. 28)

siehe auch Urteil des Bundesverfassungsgerichts
vom 15. Januar 1958 1 BvR 400/51

Sniffing beim ISP: Bsp. Carnivore



Sniffing beim ISP: Bsp. ~~Carnivore~~

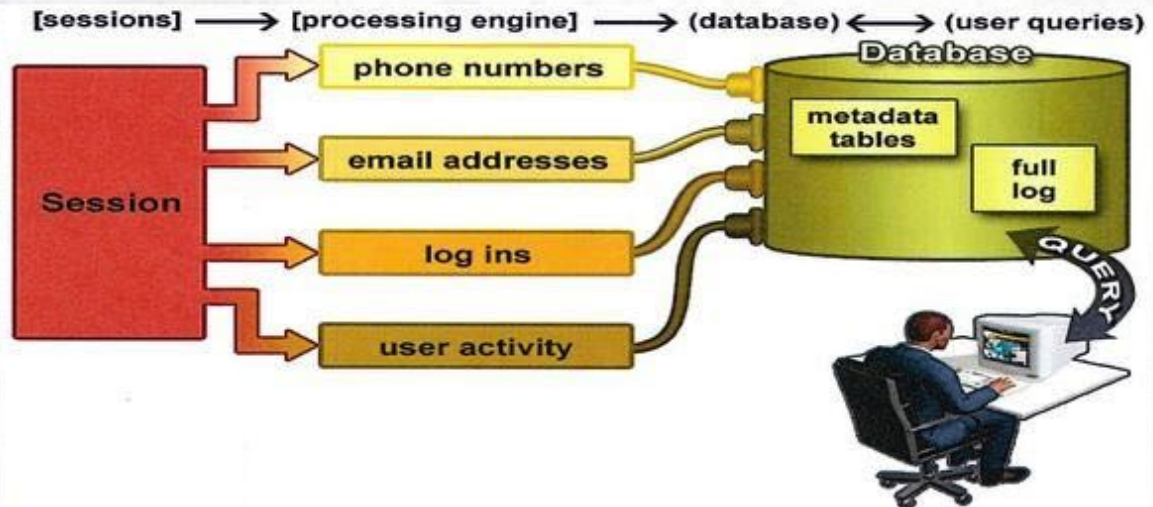
Datenbank des Überwachungs

Quelle: Wikimedia

What XKS does with the Sessions

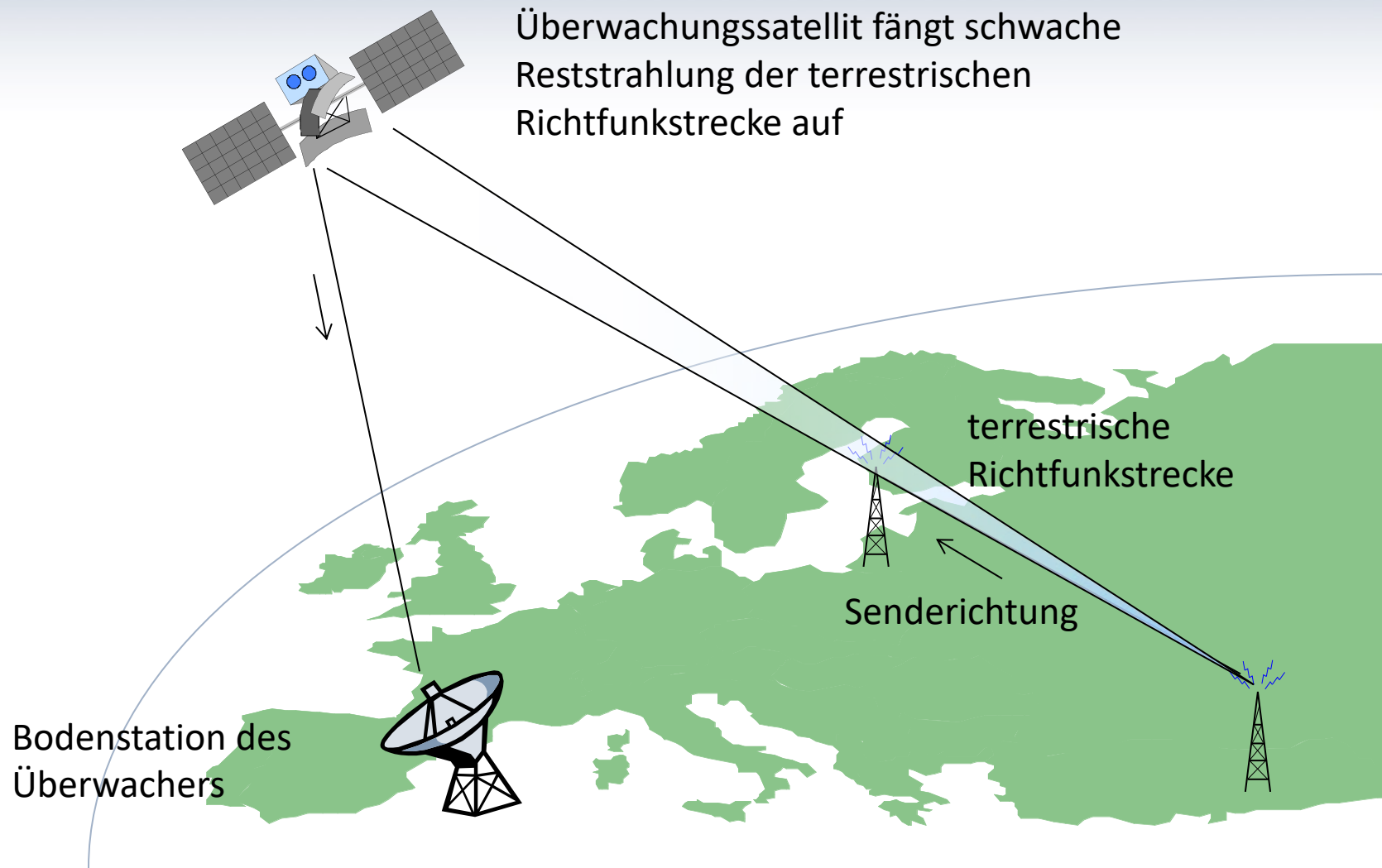


Plug-ins extract and index metadata into tables



TOP SECRET//COMINT//REL TO USA, AUS, CAN, GBR, NZL

Sniffing: Beispiel ECHELON



ECHELON

■ Das EU-Parlament über das globale Überwachungssystem ECHELON:

- «... daß nunmehr kein Zweifel mehr daran bestehen kann, daß das System nicht zum Abhören militärischer, sondern zumindest privater und wirtschaftlicher Kommunikation dient, ...»
- «... ihre Bürger und Unternehmen über die Möglichkeit zu informieren, daß ihre international übermittelten Nachrichten unter bestimmten Umständen abgefangen werden; besteht darauf, daß diese Information begleitet wird von praktischer Hilfe bei der Entwicklung und Umsetzung umfassender Schutzmaßnahmen, auch was die Sicherheit der Informationstechnik anbelangt; ...»

Bericht über die Existenz eines globalen Abhörsystems für private und wirtschaftliche Kommunikation (Abhörsystem ECHELON) (2001/2098 (INI)). EU Parlament, Nichtständiger Ausschuss über das Abhörsystem Echelon, Sitzungsdocument A5-0264/2001, Teil 1, 11. Juli 2001.

ECHELON

- Bad Aibling Interception facility of the ECHELON system



Source: <http://ig.cs.tu-berlin.de/w2000/ir1/referate2/b-1a/>

Social networks and personal data – the «Strava Heatmap» case

- Fitness tracker website publishes favourite running paths of their users
- US military personnel was (officially) equipped with fitness tracking devices
- Public heatmap discloses secret locations of military bases



Nathan Ruser @Nrg8000 · 27. Jan.

Not just US bases. Here is a Turkish patrol N of Manbij

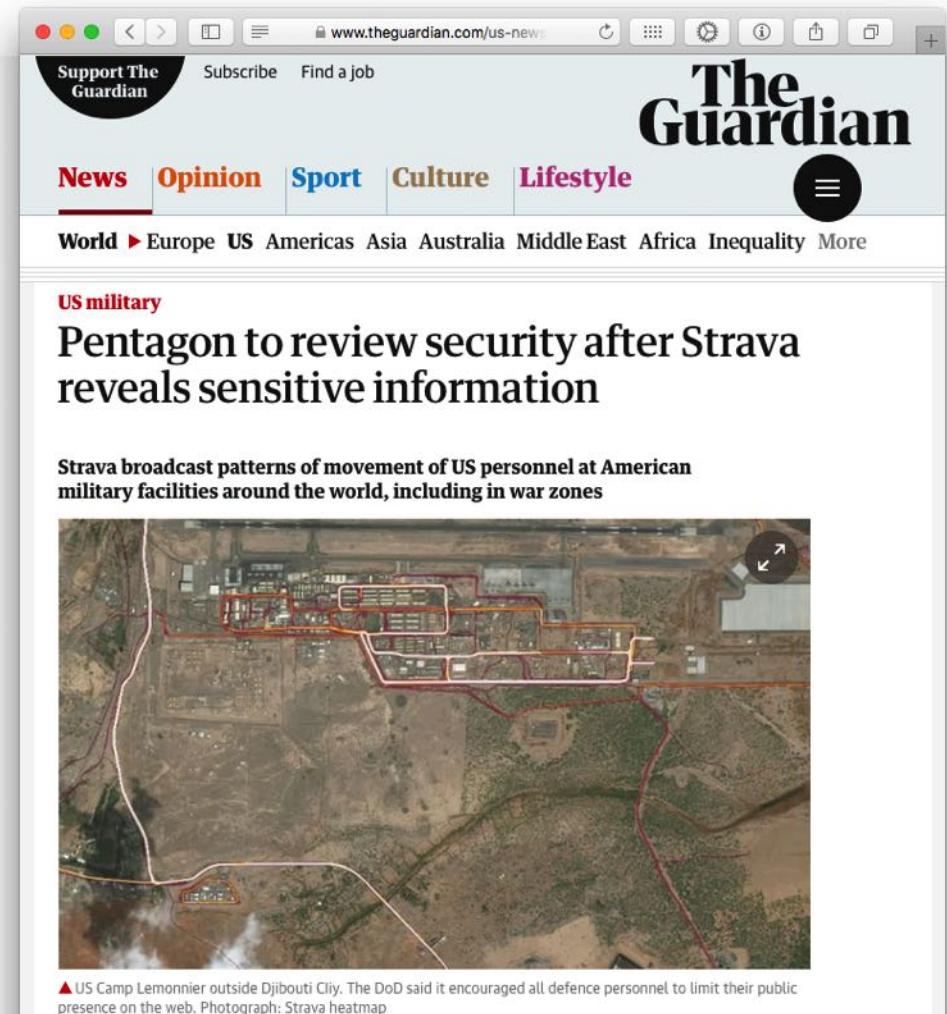


7 138 231

Sources:

<https://twitter.com/Nrg8000/status/957318498102865920>

12 <https://www.theguardian.com/us-news/2018/jan/29/pentagon-strava-fitness-security-us-military>



Anonymized data...

...can reveal comm. relations.



David Andrew Finer: What Insights Do Taxi Rides Offer into Federal Reserve Leakage? Working Paper, Booth School of Business, University of Chicago, March 2018. <https://research.chicagobooth.edu/-/media/research/stigler/pdfs/workingpapers/18whatinsightsdotaxiridesofferintofederalreserveleakage.pdf>

politico.com

POLITICO

PRO

U.S. Edition

URL: <https://www.politico.com/story/2018/03/05/what-taxi-data-shows-about-the-feds-contact-with-bankers-383751>

What taxi data shows about the Fed's contact with bankers

By VICTORIA GUIDA | 03/05/2018 12:59 PM EST

Share on Facebook

Share on Twitter

Contact between the Federal Reserve Bank of New York and six of the largest U.S. banks seems to increase around the Fed's key interest-rate-setting meetings, according to a new academic study that raises questions about whether this could give top Wall Street institutions an unfair competitive edge.

The study, from the University of Chicago's Booth School of Business, examines granular data on cab rides released by New York's taxi regulator. It singles out lunchtime trips between the New York Fed and the major offices of six banks: Goldman Sachs, Citigroup, JPMorgan Chase, Morgan Stanley, Bank of New York Mellon and Bank of America.

It also includes potential off-site meetups by factoring in "coincidental drop-offs," where someone from the New York Fed and someone from a bank each appeared to be dropped off at the same location around the same time.

Lunchtime coincidental drop-offs happened about 50 percent more often between when an important meeting of the policy-making Federal Open Market Committee started through the following week, according to the study written by David Andrew Finer. That's an average of about 1.2 more taxi rides per meeting.

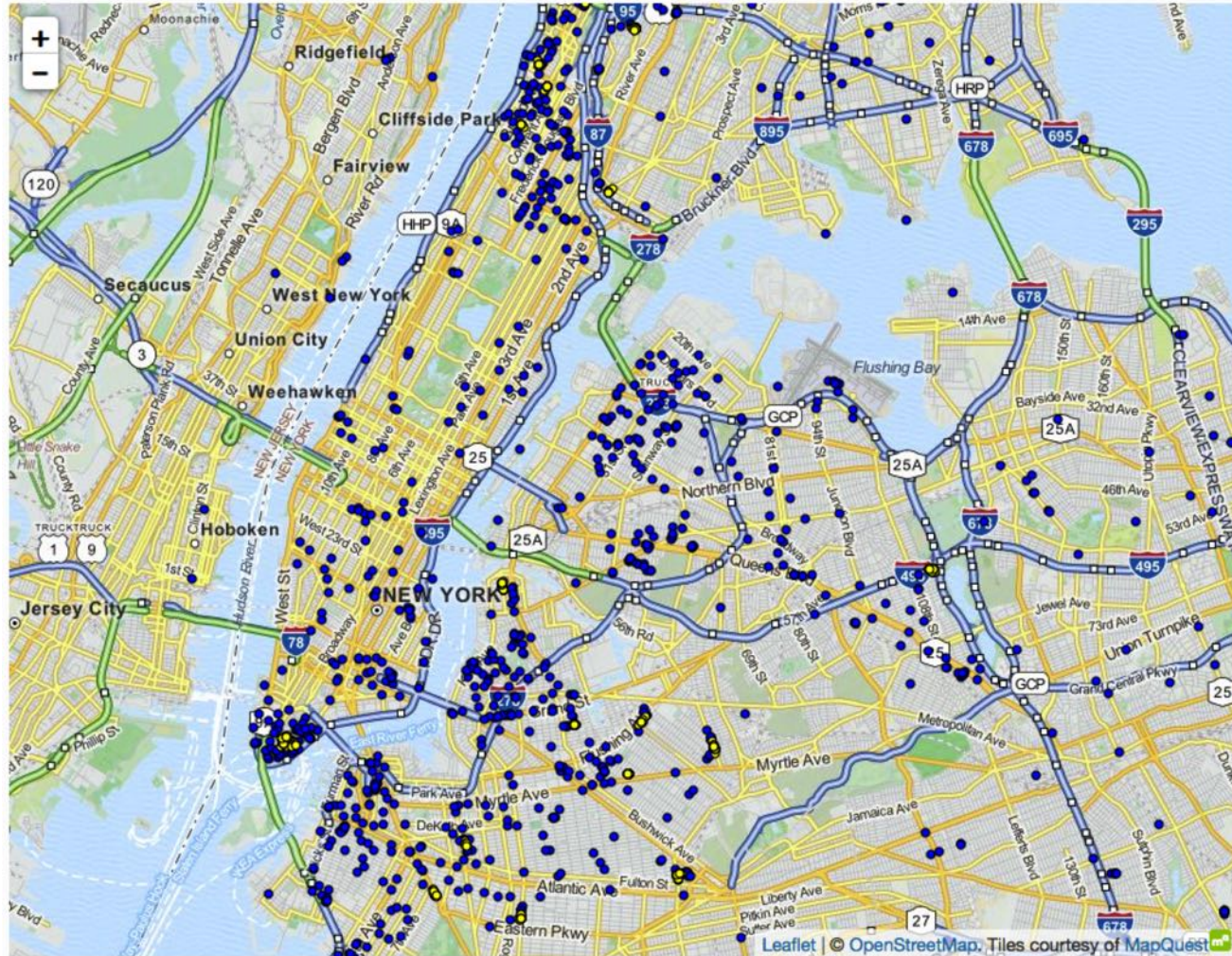
"I cannot conclusively demonstrate a link between rides and face-to-face meetings, but evidence that individuals are in very close proximity to each other more often around FOMC meetings would complement more indirect evidence of regular informal communication," the study says. It examines taxi data between 2009, when data was first made available, and 2014, before ride shares like Uber and Lyft became popular.

Pseudonymized data...

...can reveal sensitive location information.

20 GBytes of pseudonymized data

170 million taxi rides in New York



Drop-off locations for trips starting at Larry Flynt's Hustler Club between midnight and 6 am during 2013.

Source: <http://content.research.neustar.biz/blog/differential-privacy/stripeRaw.html>



Der Fall Cambridge Analytica

<

>

heise.de

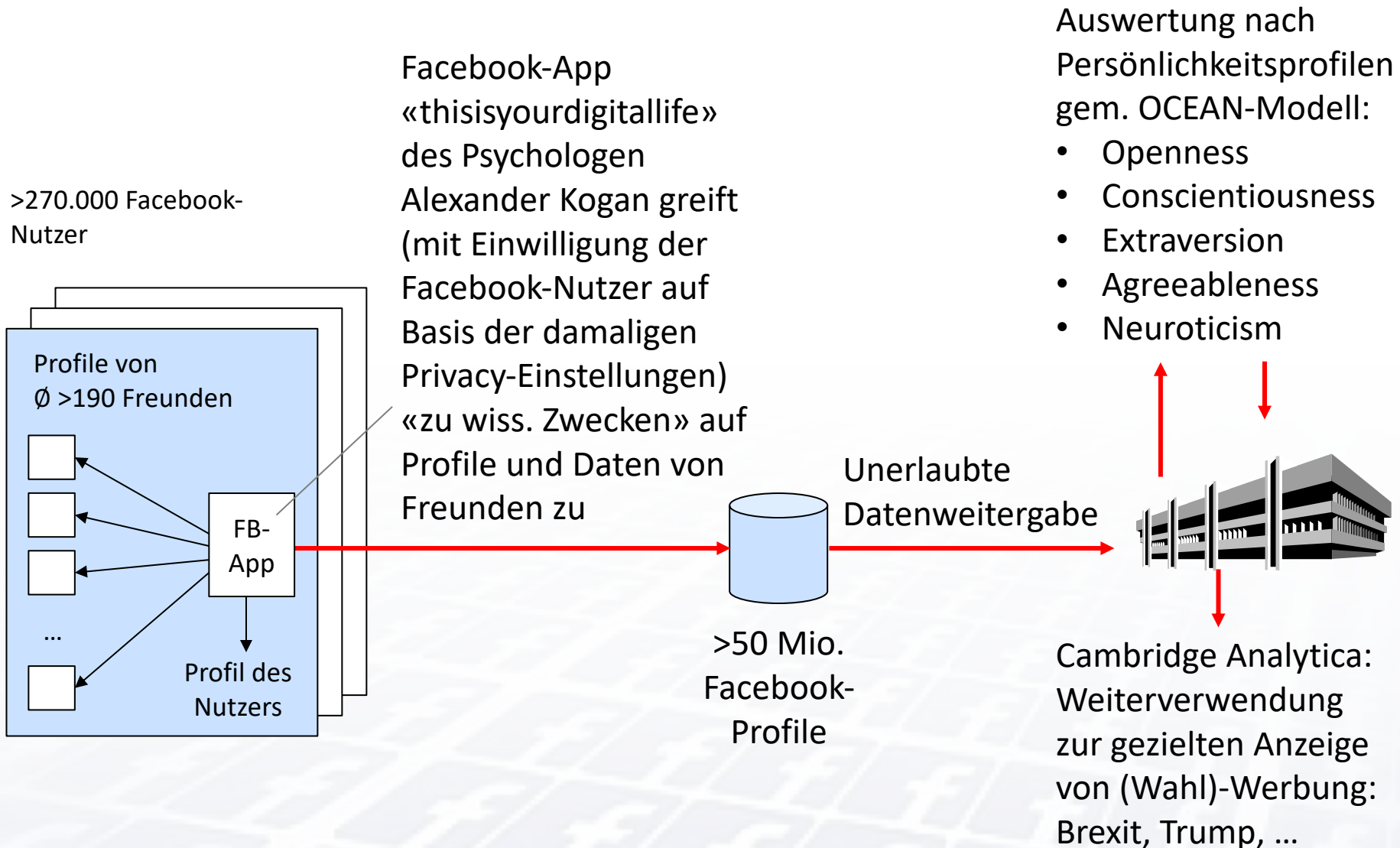
+

Facebook-Datenskandal

Die englische Datenanalyse-Firma Cambridge Analytica hat sich während des US-Wahlkampfes unerlaubt Zugang zu Daten von mehr als 50 Millionen Facebook-Nutzern verschafft. Mit den Informationen soll die Firma geholfen haben, Anhänger des heutigen US-Präsidenten Donald Trump zu mobilisieren und zugleich potenzielle Wähler der Gegenkandidaten Hillary Clinton vom Urnengang abzuhalten. Mithilfe der Nutzerprofile wurden im sozialen Netzwerk gezielt Botschaften als Werbung ausgespielt.



Der im März 2018 bekannt gewordene Datenskandal ist aber offenbar nur die Spitze eines Eisbergs. Laut einem ehemaligen Facebook-Manager habe das Social Network keinerlei Kontrolle über abgeflossene Nutzerdaten.



1. Ort
2. Alter
3. Generation
4. Geschlecht
5. Sprache
6. Bildungsniveau
7. Ausbildungsbereich
8. Schule
9. ethnische Zugehörigkeit
10. Einkommen und Eigenkapital
11. Hausbesitz und -typ
12. Hauswert
13. Grundstücksgröße
14. Hausgröße in Quadratmeter
15. Jahr, in dem das Haus gebaut wurde
16. Haushaltszusammensetzung
17. Nutzer, die innerhalb von 30 Tagen ein Jubiläum haben
18. Nutzer, die von der Familie oder Heimatstadt entfernt sind



Say you're scrolling through your Facebook Newsfeed and you encounter an ad so eerily well-suited, it seems someone has possibly read your brain.

https://www.washingtonpost.com/news/the-intersect/wp/2016/08/19/98-personal-data-points-that-facebook-uses-to-target-ads-to-you/?noredirect=on&utm_term=.e99142ea2597

<https://netzpolitik.org/2016/98-daten-die-facebook-ueber-dich-weiss-und-nutzt-um-werbung-auf-dich-zuzuschneiden/>

Facebooks 98 Datenpunkte zum Targeting

Washington Post

19. Nutzer die mit jemandem befreundet sind, der einen Jahrestag hat, frisch verheiratet oder verlobt ist, gerade umgezogen ist oder bald Geburtstag hat
20. Nutzer in Fernbeziehungen
21. Nutzer in neuen Beziehungen
22. Nutzer mit neuen Jobs
23. Nutzer, die frisch verlobt sind
24. Nutzer, die frisch verheiratet sind
25. Nutzer, die vor Kurzem umgezogen sind
26. Nutzer, die bald Geburtstag haben
27. Eltern
28. Werdende Eltern
29. Mütter in Typen unterteilt („Fußball, trendy“ etc.)
30. Nutzer, die sich wahrscheinlich politisch betätigen
31. Konservative und Liberale
32. Beziehungsstatus
33. Arbeitgeber
34. Branche
35. Berufsbezeichnung
36. Art des Büros
37. Interessen
38. Nutzer, die ein Motorrad besitzen
39. Nutzer, die planen, ein Auto zu kaufen (welche Art/Marke, und wann)
40. Nutzer, die kürzlich Autoteile oder Zubehör gekauft haben
41. Nutzer die wahrscheinlich Autoteile oder Service benötigen
42. Art und Marke des Autos, das man fährt
43. Jahr, in dem das Auto gekauft wurde
44. Alter des Autos
45. Wieviel Geld der Nutzer vermutlich für sein nächstes Auto ausgeben wird
46. Wo der Nutzer vermutlich sein nächstes Auto kaufen wird
47. Wieviele Mitarbeiter die eigene Firma hat
48. Nutzer, die kleine Unternehmen haben
49. Nutzer, die Manager oder Führungskräfte sind
50. Nutzer, die für wohltätige Zwecke gespendet haben (unterteilt nach Art)

Facebooks 98 Datenpunkte zum Targeting

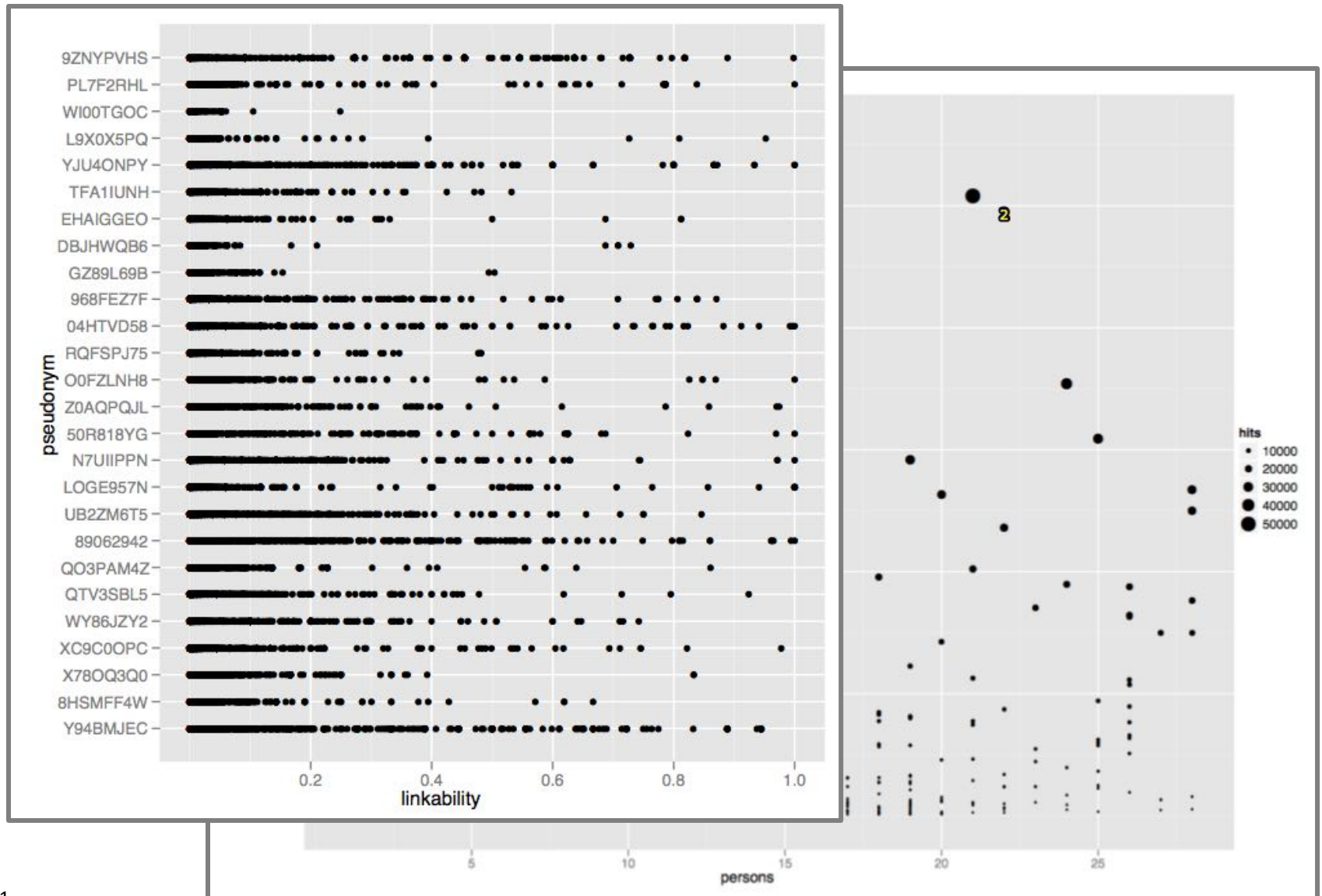
Washington Post

51. Betriebssystem
52. Nutzer, die Browserspiele spielen
53. Nutzer, die eine Spielekonsole besitzen
54. Nutzer, die eine Facebook-Veranstaltung erstellt haben
55. Nutzer, die Facebook-Payments benutzt haben
56. Nutzer, die mehr als üblich per Facebook-Payments ausgegeben haben
57. Nutzer, die Administrator einer Facebookseite sind
58. Nutzer, die vor Kurzem ein Foto auf Facebook hochgeladen haben
59. Internetbrowser
60. Emailanbieter
61. „Early Adopters“ und „late Adopters“ von Technologien
62. Auswanderer (sortiert nach dem Ursprungsland)
63. Nutzer, die einer Genossenschaftsbank, einer nationalen oder regionalen Bank angehören
64. Nutzer, die Investoren sind (sortiert nach Typ der Investition)
65. Anzahl der Kredite
66. Nutzer, die aktiv eine Kreditkarte benutzen
67. Typ der Kreditkarte
68. Nutzer, die eine Lastschriftkarte haben
69. Nutzer, die Guthaben auf der Kreditkarte haben
70. Nutzer, die Radio hören
71. Bevorzugte TV-Shows
72. Nutzer, die ein mobiles Gerät benutzen (nach Marke aufgeteilt)
73. Art der Internetverbindung
74. Nutzer, die kürzlich ein Tablet oder Smartphone gekauft haben
75. Nutzer, die das Internet mit einem Smartphone oder einem Tablet benutzen
76. Nutzer, die Coupons benutzen
77. Arten von Kleidung, die der Haushalt des Nutzers kauft

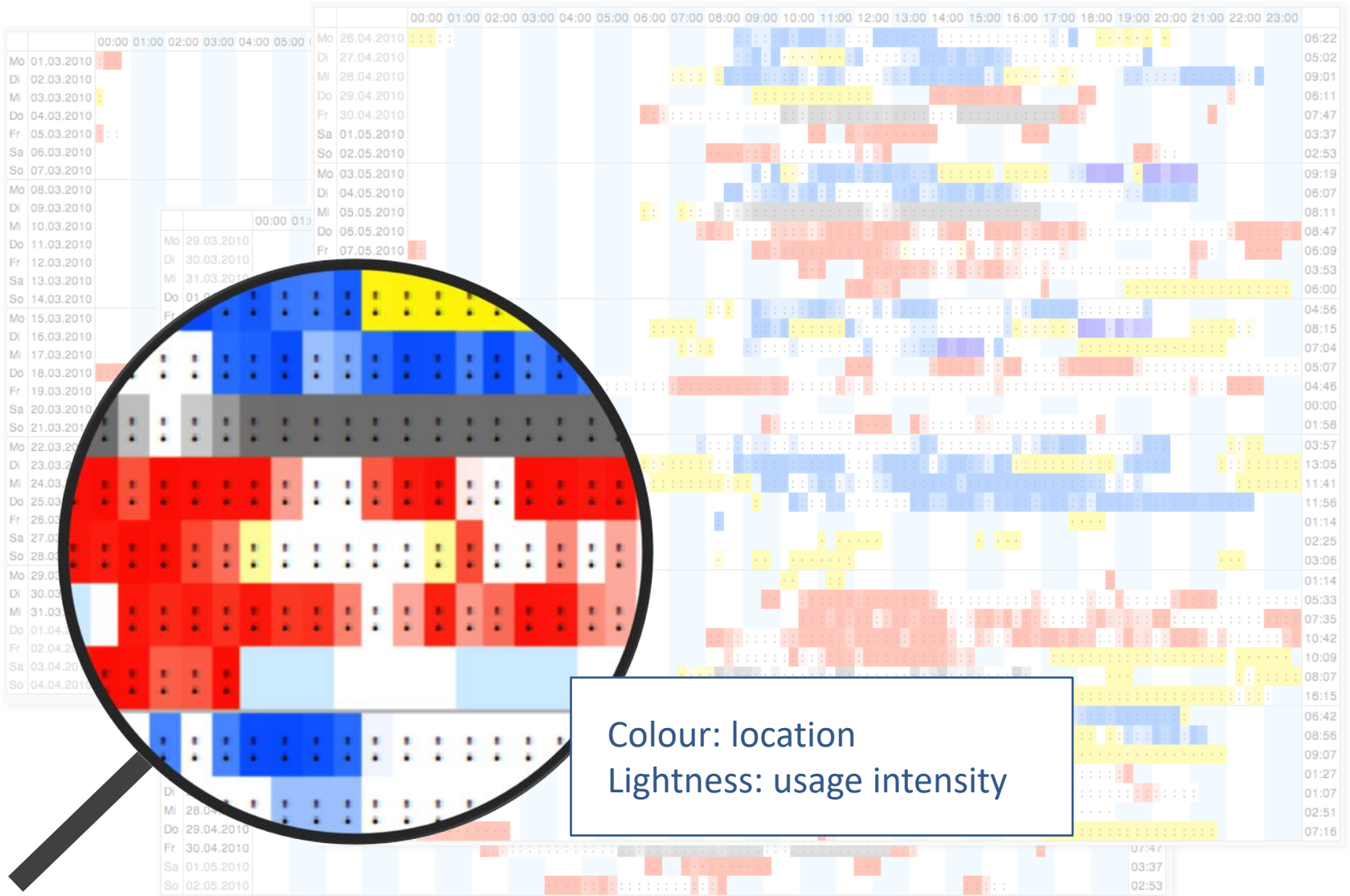
Facebooks 98 Datenpunkte zum Targeting

Washington Post

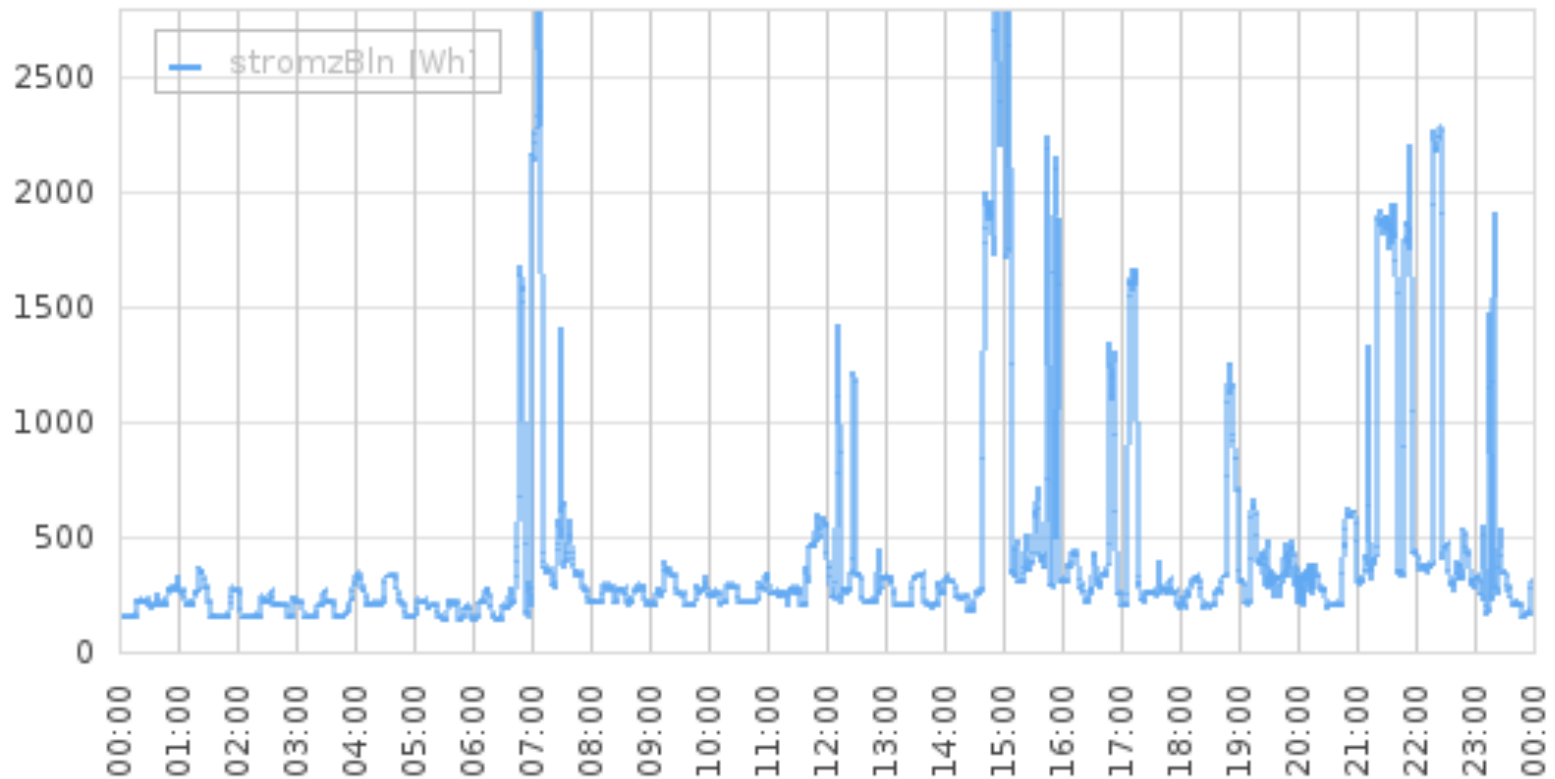
78. Die Zeit im Jahr, in der der Haushalt des Nutzers am meisten einkauft
79. Nutzer, die „sehr viel“ Bier, Wein oder Spirituosen kaufen
80. Nutzer, die Lebensmittel einkaufen (und welche Art)
81. Nutzer, die Kosmetikprodukte kaufen
82. Nutzer, die Medikamente gegen Allergien und Schnupfen/Grippe, Schmerzmittel und andere nicht-verschreibungspflichtige Arzneimittel einkaufen
83. Nutzer, die Geld für Haushaltsgegenstände ausgeben
84. Nutzer, die Geld für Produkte für Kinder oder Haustiere ausgeben (und welche Art von Haustier)
85. Nutzer, deren Haushalt mehr als üblich einkauft
86. Nutzer, die dazu neigen online (oder offline) einzukaufen
87. Arten von Restaurants, in denen der Nutzer isst
88. Arten von Läden, in denen der Nutzer einkauft
89. Nutzer, die „empfänglich“ für Angebote von Firmen sind, die Online-Autoversicherungen, Hochschulbildung oder Hypotheken, Prepaid-Debitkarten und Satellitenfernsehen anbieten
90. Wie lange der Nutzer sein Haus bereits bewohnt
91. Nutzer, die wahrscheinlich bald umziehen
92. Nutzer, die sich für Olympische Spiele, Cricket oder Ramadan interessieren
93. Nutzer, die häufig verreisen (geschäftlich oder privat)
94. Nutzer, die zur Arbeit pendeln
95. Welche Art von Urlaub der Nutzer bucht
96. Nutzer, die kürzlich von einem Ausflug zurückkommen
97. Nutzer, die kürzlich eine Reise-App benutzt haben
98. Nutzer, die ein Ferienwohnrecht haben



Usage timelines and ip-geo-tagging



Stromverbrauch verrät Infos über persönliche Lebensverhältnisse



Broadcast

■ Das war damals...



- Zeitung lesen
- Radio über Antenne hören
- Fernsehen über Breitbandverteilkabel

■ Verteilung (Broadcast) + implizite Adressierung

- Technik zum Schutz des Empfängers
- Alle Teilnehmer erhalten alles
- Lokale Auswahl
- Es bleibt verborgen, welchen Inhalt der Nutzer konsumiert

Broadcast

■ Heute: (Vermittlungsnetze)

- Video on Demand
- Internet-Radio
- Zeitungen online

- Plötzlich stehen Nutzungsdaten zur Verfügung.
- Der Kunde wird gläsern.

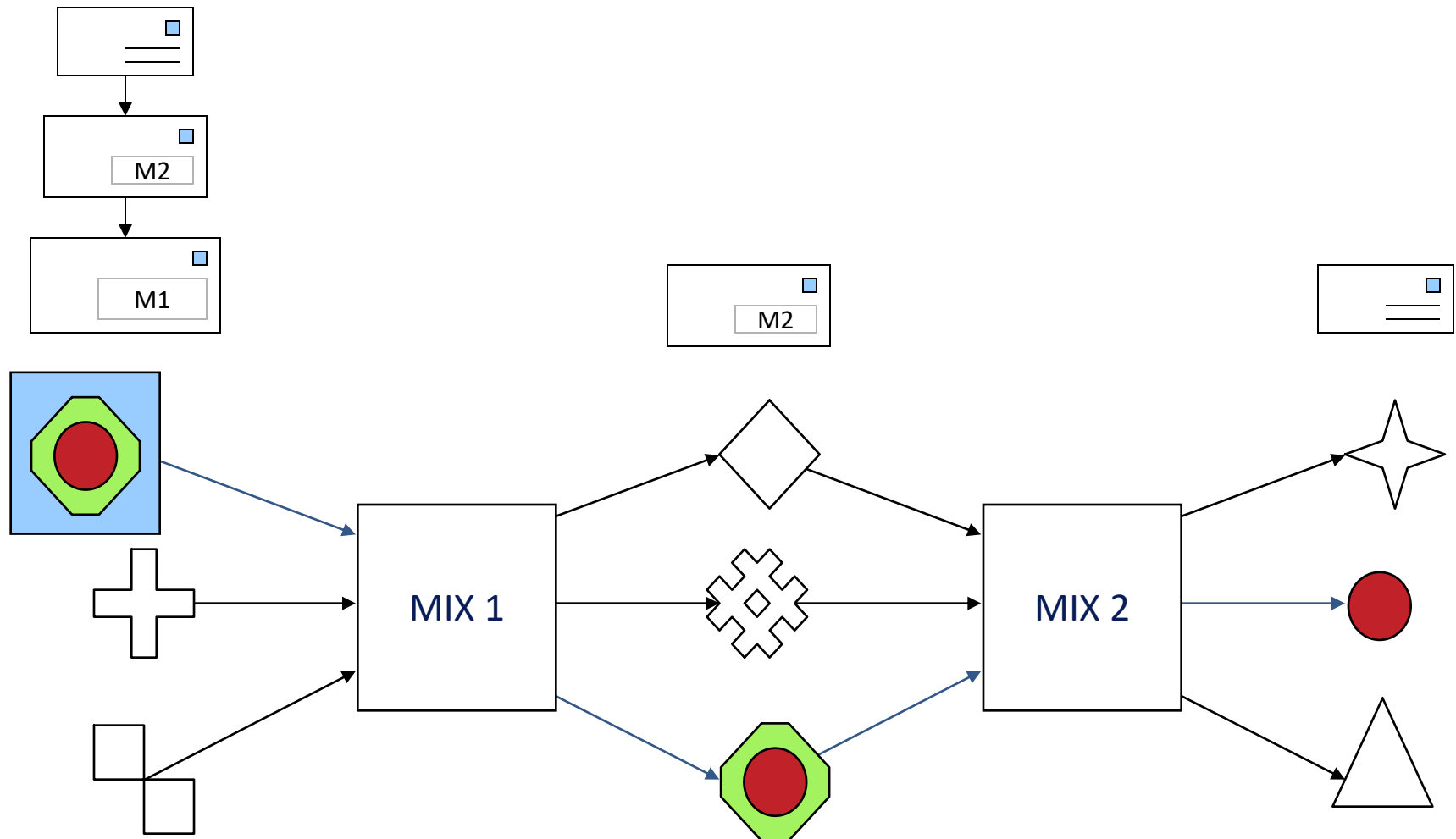
• Damals: (Broadcast)

- Zeitung lesen
- Radio über Antenne hören
- Fernsehen über Breitbandverteilkabel

■ Verteilung (Broadcast) + implizite Adressierung

- Technik zum Schutz des Empfängers
- Alle Teilnehmer erhalten alles
- Lokale Auswahl
- Es bleibt verborgen, welchen Inhalt der Nutzer konsumiert

- System zum Schutz von Kommunikationsbeziehungen bei vermittelter Kommunikation



Tor und JonDonym: Anonymes Surfen

- Schutz auch vor dem Betreiber des Anonymisierungsdienstes
 - <https://www.torproject.org>
 - <https://www.anonym-surfen.de>
- Besonders einfache Verwendung beim anonymen Websurfen mit den integrierten Browsern
 - Tor Browser Bundle
 - JonDoFox





Prof. Dr. Hannes Federrath
Fachbereich Informatik
Universität Hamburg
Vogt-Kölln-Straße 30
D-22527 Hamburg

Telefon +49 40 42883 2358

E-Mail federrath@informatik.uni-hamburg.de

<https://svs.informatik.uni-hamburg.de>