SVRV Sachverständigenrat für Verbraucherfragen

Datenschatten - Verbraucherfragen im digitalen Zeitalter

Tactical Technology Collective

Studien und Gutachten im Auftrag des Sachverständigenrats für Verbraucherfragen

Januar 2016

Berlin, Januar 2016
ISSN 2365-8436

Herausgeber:

Sachverständigenrat für Verbraucherfragen
beim Bundesministerium der Justiz und für Verbraucherschutz
Mohrenstraße 37
10117 Berlin

Telefon: +49 (0) 30 18 580-0
Fax: +49 (0) 30 18 580-9525
E-Mail: info@svr-verbraucherfragen.de
Internet: www.svr-verbraucherfragen.de

Diese Veröffentlichung ist im Internet abrufbar.

Mitglieder des SVRV

Prof. Dr. Lucia Reisch (Vorsitzende)
Professorin für Interkulturelle Konsumforschung und europäische Verbraucherpolitik an der Copenhagen Business School

Dr. Daniela Büchel (stellv. Vorsitzende)
Mitglied der Geschäftsleitung REWE für die Bereiche Human Resources und Nachhaltigkeit

Prof. Dr. Gerd Gigerenzer
Direktor der Abteilung „Adaptives Verhalten und Kognition“ und des Harding-Zentrums für Risikokompetenz am Max-Planck-Institut für Bildungsforschung in Berlin

Helga Zander-Hayat
Leiterin des Bereichs Markt und Recht bei der Verbraucherzentrale Nordrhein-Westfalen

Prof. Dr. Gesche Joost
Professorin für das Fachgebiet Designforschung an der Universität der Künste und Internetbotschafterin der Bundesregierung im Gremium der „Digital Champions“ der EU

Prof. Dr. Hans-Wolfgang Micklitz
Professor für Wirtschaftsrecht am Europäischen Hochschulinstitut in Florenz

Prof. Dr. Andreas Oehler
Professor für Finanzwirtschaft an der Universität Bamberg und Direktor der Forschungsstelle Verbraucherfinanzen und Verbraucherbildung

Prof. Dr. Kirsten Schlegel-Matthies
Professorin für Haushaltswissenschaft an der Universität Paderborn

Prof. Dr. Gert G. Wagner
Professor für Empirische Wirtschaftsforschung und Wirtschaftspolitik an der Technischen Universität Berlin, Vorstandsmitglied des Deutschen Instituts für Wirtschaftsforschung und Max Planck Fellow am MPI für Bildungsforschung

Mitarbeitende des SVRV

Leiter der Geschäftsstelle: Thomas Fischer

Wissenschaftlicher Stab der Geschäftsstelle: Dr. Irina Domurath, Dr. Christian Groß

TACTICAL TECHNOLOGY COLLECTIVE

turning information into action

Datenschatten - Verbraucherfragen im digitalen Zeitalter

Bericht: Dezember 2015

Einführung

Als Teil des Berichts zum Nutzungsverhalten im digitalen Zeitalter hielt Tactical Tech einen praxisorientierten Workshop ab, der auf Fragen über das Bewusstsein deutscher Verbraucher/innen in Bezug auf Datenschatten, Datenspuren und die Wege, seine Daten zu schützen, eingehen sollte. Die Anliegen und Fragen, die vonseiten der Verbraucher/innen in Bezug auf ihre Datenschatten während des Workshops aufkamen, wurden gesammelt und analysiert. Die darauf basierenden Resultate werden in diesem Bericht vorgestellt.

Der Workshop fußte auf dem Grundsatz Tactical Techs, dass es innerhalb einer Informationsgesellschaft wichtig ist, Verbraucher/innen mit den Fähigkeiten und dem Wissen auszustatten, sich innerhalb der Datenlandschaft bewegen zu können und dabei fundierte Entscheidungen treffen zu können, sowohl jetzt als auch in den kommenden Jahren. Wir glauben, es ist wichtig, bestimmte Konzepte und Werkzeuge in die alltäglichen Abläufe und Anliegen einzubinden, die Verbraucher/innen haben können. Diese Art von Workshop gibt Verbraucher/innen die Möglichkeit, ihren Anliegen in ihren eigenen Worten auf Basis ihrer eigenen Erfahrungen Ausdruck zu verleihen. Darauf aufbauend wird ihnen die Möglichkeit gegeben, ihre eigenen Datenschatten zu skizzieren und spezielle Belange, die mit Handel, Gesundheit und Finanzen in Zusammenhang stehen, hervorzubringen.

Ablauf

Tactical Tech hat einen „Offenen Aufruf“ an deutsche Verbraucher/innen herausgegeben, an dem Workshop teilzunehmen. Teilnahmeinteressierte konnten sich per E-Mail bewerben, in der sie ihren Namen genannt haben und einen kurzen Absatz zu ihrer Motivation verfasst haben, so dass wir ihren Hintergrund und den Grad ihrer Kenntnisse in Bezug auf Datenpolitik einschätzen konnten. Dies mündete in einen eintägigen Workshop, bei dem mithilfe zahlreicher Aktivitäten und Diskussionen die Anliegen deutscher Verbraucher/innen Ausdruck fanden.

Demographie

Es gab 20 Teilnehmende, 9 männliche und 11 weibliche.
Die Altersspanne verlief geschätzt von 25-45, wobei ca. 75% zwischen 30 und 35 waren.
Berufsstände die vertreten waren umfassten einen Journalisten, einen Professoren, einen Linguisten, Designer, Community Organiser und Studierende, deren Fächer von Reproduktiven Rechten bis zu Sicherheitspolitik reichten. 25% der Teilnehmenden arbeiteten direkt auf einem technologieaffinen Gebiet und verfügten über technische Vorkenntnisse.

Tagesplan / Erklärung: warum wir diese Übungen ausgesucht haben

10:00-10:30 Einführung, Tagesplan und Vorstellungsrunde

10:30-11:00 Post-it-Übung: Was glaubst du ist wichtig in Bezug auf Daten?

11:00-11:45 Den eigenen Browserverlauf nachzeichnen

11:45-12:00 Kaffee

12:00-13:20 Rekapitulation der Browser-Übung und Erklärung grundlegender Konzepte

13:20-14:30 Mittagessen

14:30-15:45 World Café: Gesundheit, Finanzen, Online-Shopping, Standort-/Mobildaten

15:45-16:30 Praktische Wege, den Datenschutz zu erhöhen und Zusammenfassung

Übungen

10:00-10:30 *Einführung, Tagesplan und Vorstellungsrunde*

Durchführung: Tactical Tech wird vorgestellt, die Zielsetzung des Workshops vermittelt und der Tagesablauf präsentiert. Anschließend wurden die Teilnehmenden aufgefordert, sich vorzustellen und zu erzählen, warum sie am Workshop teilnehmen und wie sie ihren eigenen Datenschatten einschätzen.

Ziel: Die Teilnehmenden können ihre Intentionen in eigenen Worten vermitteln und innerhalb der ersten 30 Minuten wurde allen erlaubt, sich offen auszutauschen und ihrer eigenen Stimme Ausdruck zu verleihen.

Die Erwartungen der Teilnehmenden lassen sich wie folgt zusammenfassen: zu verstehen, welche Art von Daten gesammelt werden, mehr über dieses Thema zu erfahren und zu lernen, wie man mit anderen Menschen über das Thema Datenschatten sprechen kann. Gleichzeitig sollten praktische Wege gefunden werden, die Verbreitung der eigenen Daten besser kontrollieren zu können.

10:30-11:00 *Post-it-Übung: Was glaubst du ist wichtig in Bezug auf Daten?*

Durchführung: Teilnehmende bekamen Post-its ausgeteilt und wurden ermutigt, jeweils eine Idee oder ein Anliegen auf ein Post-it zu schreiben. Sobald sie alle Zettel ausgefüllt hatten, wurden diese an die Wand geklebt. Danach haben die Teilnehmenden die einzelnen Zettel neu angeordnet und sie dabei in sich abzeichnende Kategorien unterteilt.

Ziel: Diese Übung sollte Aufschluss darüber liefern, welche Ideen die Menschen in Bezug auf Daten beschäftigen und welche Probleme sie sehen. Außerdem sollte die Sprache untersucht werden, mithilfe derer die Teilnehmenden diese Anliegen beschreiben und welche Vorkenntnisse bereits vorhanden sind.

Die Gruppe hat alle Post-its in Kategorien unterteilt, die sie selbst definiert haben, darunter *Firmen*, *Technisches*, *Überwachung*, *Kuration*, *Vernetzung*, soziale und ethische Belange.

Eine vollständige Dokumentierung findet sich in Anhang 1

Einige Kernpunkte innerhalb dieser Kategorien umfassten u.a.:

Firmen: Die Post-its beschäftigten sich mit der Verstrickung von Staaten und der Industrie, Datenaustausch mit Dritten und individualisierter Werbung.

Überwachung: Teilnehmende schrieben über „Überwachung als Geschäftsmodell im Internet" und stellten Fragen über Identitätsdiebstahl und inwiefern das Bildungssystem sich verändert, um die digitale Welt mit einzuschließen.

Vernetzung: Verschiedene Punkte über die Verbindung zwischen Geräten und verschiedenen Datenquellen: „Wie viel kostet mein Schatten?" oder „Verwechslung: Auf einer No-Fly-Liste landen, weil jemand meine Daten vertauscht hat."

Soziales: Fragen über den Einfluss und die Langlebigkeit unserer Daten. „Wenn ich einen Account lösche (Facebook, Pinterest, Twitter, Instagram etc.), verschwindet er dann wirklich?" und „Was passiert, wenn mein E-Mail-Account gehackt wird?". Es tauchten auch Fragen darüber auf, ob es so etwas wie eine soziale Etikette gäbe, wenn Freunde untereinander Daten austauschen.

Kuration: Diese Kategorie umfasste zwei Seiten. Einerseits kam die Frage auf, ob wir als Nutzer/innen in der Lage wären, unseren eigenen digitalen Schatten zu kuratieren, indem wir die Informationen kontrollieren, die wir online stellen und andererseits, welche Informationen von Datenhändlern genutzt werden, um ein Bild von uns zu zeichnen.

In der Rekapitulation erwähnten Teilnehmende, dass es Schnittmengen zwischen den verschiedenen Kategorien gebe. Während wir die Zettel angeordnet haben, schienen sie alle eigenen Zweigen anzugehören, aber es gibt große Überschneidungen. Es kam außerdem der Wunsch auf, mehr über die eingesetzten Technologien zu erfahren und über die Arten von Daten, die gesammelt werden und inwiefern diese Daten benutzt werden. Viele Fragen betrafen die Kontrollmöglichkeiten in Bezug auf die eigenen Daten und ob es möglich wäre, Datenspuren zu löschen.

11:00-11:45 *Den eigenen Browserverlauf nachzeichnen*

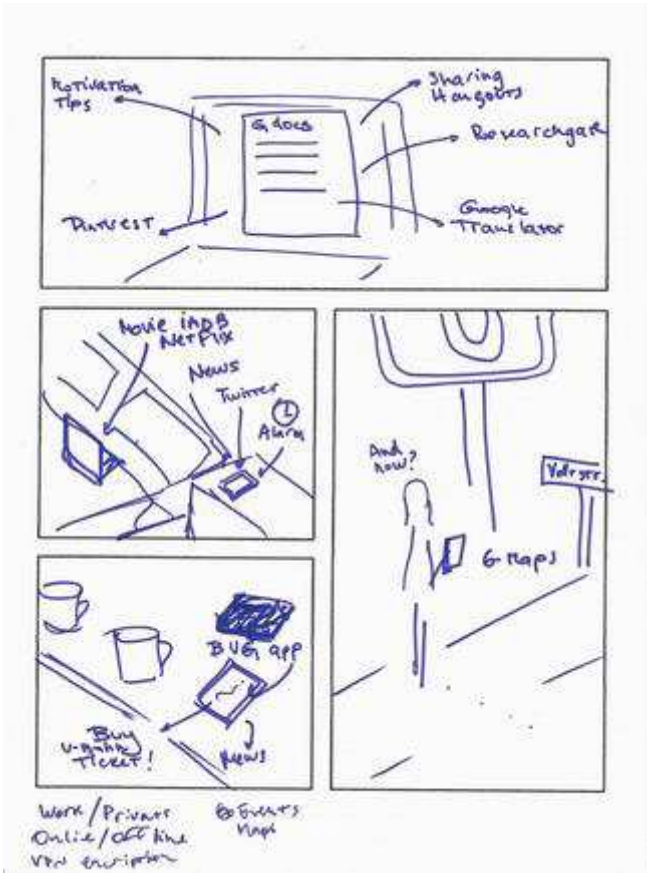
Durchführung: Zeichenpapiere wurden ausgeteilt und die Teilnehmenden gebeten, ihren Browserverlauf nachzuzeichnen, entweder den des Tages zuvor oder einen vor einigen Tagen. Anschließend wurden die Teilnehmenden in Gruppen von jeweils vier unterteilt, um ihren Browserverlauf zu besprechen, wo die Unterschiede lagen, wo es Gemeinsamkeiten gab, Aspekte, die hervorstachen und welche Anliegen damit verbunden sind. Jede der Kleingruppen gab im Anschluss an diese Diskussion einen Bericht an die gesamte Gruppe.

Ziel: Diese Übung sollte dabei helfen, abstrakte Konzepte konkreter und persönlicher zu machen.

Die meisten Zeichnungen stellten konkrete Produkte und Aktivitäten in einen Zusammenhang mit dem eigenen Browserverlauf, so z.B.:

- Nachrichten und Medien
- Als Planungsmöglichkeit für Treffen und Events
- Recherche und Lesen von Artikeln
- Online-Banking und Finanzplanung
- Schule
- Online-Shopping: besonders Amazon und Zalando
- E-Mail
- Soziale Netzwerke
- Bestimmte kommerzielle Dienste: Google, Gmail, Google Maps, Google-Suche, Google Docs, Google Hangout, Google-Übersetzer, Instagram, Facebook, WhatsApp, Twitter, Pinterest
- Reisen
- Unterhaltung: Musik, Spiele, Videos, Netflix

Einige Zeichnungen offenbarten einen emotionaleren Bezug zum Browser und inwiefern das Internet zur Erweiterung des eigenen Lebens geworden ist. Es gab außerdem Kommentare wie „Ich habe alles vergessen, was ich gemacht habe“ oder eine Teilnehmerin, die einen Tag skizziert hat, an dem sie krank war und das Internet nicht als Blackbox gebraucht hat.



Eine vollständige Dokumentierung findet sich in Anhang 2

Aus den Berichten der Kleingruppen ging hervor, dass es sich nicht nur um einen einzelnen Browserverlauf handelt, sondern sich dieser aus der Nutzung verschiedener Browser (Firefox, Chrome, Tor) und verschiedener Geräte (Computer, Handy und Tablet) zusammensetzt. Außerdem war bei den Aktivitäten entscheidend, ob sie mit dem Beruf oder Freizeitbeschäftigungen zusammenhängen.

Es traten Fragen auf, wie sehr wir uns darüber sorgen müssten, dass Browser unseren Webseitenverlauf speichern und ob es Möglichkeiten gäbe, die Datensammlung durch Cookies und Firmen zu verhindern. Viele warfen außerdem die Frage auf, ob sich der heutige Unterricht verändere und Kindern dabei helfe, sich innerhalb digitaler Landschaften zurechtzufinden. Ob sich die Verlaufsdaten, die innerhalb des Browsers gesammelt werden mit anderen Formen des Datensammelns vergleichen ließen, bspw. in Smart Cities, und ob das grundsätzlich etwas Schlechtes sei. Einige Kleingruppen besprachen Lösungsansätze, indem andere Browser oder Tor verwendet werden, die Grundeinstellungen des Browsers verändert oder andere Suchmaschinen benutzt werden. Hierbei kam allerdings die Frage auf, ob sich diese Mühe auszahlen würde.

12:00-13:20 *Erklärung von Tactical Tech*

Nach der Browser-Übung erklärten die Veranstaltenden ausführlicher, wie sich Daten definieren lassen, wie sie erzeugt und benutzt werden. Dabei ging es zuerst um die Unterscheidung zwischen Inhalten und Metadaten und im Anschluss darum, wodurch Daten zur eigenen Person generiert werden und wie viel Kontrolle wir über diese besitzen.

1. Was sind Daten?

* Inhalte - was ist der Inhalt dieser Nachricht oder E-Mail
* Metadaten - Daten über Daten
Beispiele für Metadaten sind: Zeit, Dienstanbieter, Sender und Empfänger, IP-Adresse, Header einer E-Mail, Typ und Marke eines Geräts (Handy, Computer, Tablet, Kamera usw.), Standort und in einigen Ländern gelten auch Betreffzeilen von E-Mails als Metadaten.

2. Aufschlüsseln, welche Möglichkeiten bestehen, die eigenen Daten zu kontrollieren

Bruce Schneier nennt sechs verschiedene Abstufungen von Datenschöpfung, die von der höchsten bis zur geringsten eigenen Kontrolle über die Daten reichen.

- *Registrierungsdaten:* Daten, die angegeben werden müssen, um sich für ein Programm oder einen Service zu registrieren. Wenn man das Programm oder den Service nutzen will, muss man Daten zur Verfügung stellen. Dabei sollte beachtet werden, welche Felder optional und welche verpflichtend sind. Möchte man diese Daten nicht preisgeben, bleibt einem nur, den Dienst nicht zu nutzen.

- *Einen eigenen Dienst verwenden:* Es besteht die Möglichkeit, zu entscheiden, wer Zugriff auf den Dienst hat, wo die Daten gespeichert werden usw.

- *Einen fremden Dienst nutzen:* Benutzer/innen stellen dem Dienst bestimmte Daten allein durch die Nutzung zur Verfügung. Bspw. Inhalte, die man veröffentlicht, kommuniziert oder regelmäßig speichert.

- *Wenn andere Daten über einen erstellen:* Im Falle von Bildern, Tagging (bspw. auf Facebook), die Erwähnung des Namens, aber auch Interviews, Konferenzen und andere Veranstaltungen.

- *Verhaltensdaten:* Standortdaten. Schaut man auf sein iPhone ist ersichtlich, wie viele Standortdaten gesammelt werden und welche Verhaltensmuster aus diesen destilliert werden können. Wo wir wohnen, arbeiten etc.

- *Abgeleitete Daten:* Firmen, die Gruppenprofile erstellen und mithilfe der Charakteristika dieser Gruppen Rückschlüsse auf das Individuum ziehen. Bspw. wenn eine Teilnehmende in Neukölln lebt, werden auf Basis dieser Information bestimmte Annahmen über ihren Hintergrund und ihre Vorlieben gemacht.

14:30-15:45 *World Café: Gesundheit, Finanzen, Online-Shopping, Standort- und Mobildaten*

Ein Diskussionsformat zu Verbraucher/innenanliegen: Gesundheit, Finanzen, Online-Shopping und Mobiltelefone/Standort. Die Fragen während der Diskussion waren:

> Was sind eure Praktiken?
> Welche Probleme gibt es in Bezug auf Datenpolitik?
> Was wären mögliche Lösungsansätze?

Durchführung: Jedes Thema (Gesundheit, Finanzen, Online-Shopping und Standort-/Mobildaten) bekam eine Person pro Tisch zugeteilt, die dafür verantwortlich war, die Diskussion zu leiten. Die Teilnehmenden wurden in vier Gruppen unterteilt und jeder Gruppe ein Thema gegeben. Die Gruppen besprachen das jeweilige Thema für zehn Minuten, wonach sie zu einem anderen Thema übergingen. Jedes Mal, wenn die Gruppe zu einem neuen Thema überging, gab der Diskussionsleiter / die Diskussionsleiterin eine kurze Zusammenfassung. Nachdem alle Gruppen alle Themen diskutiert hatten, rekapitulierten die Diskussionsleitenden die Ergebnisse für alle Gruppen.

Ziel: Das Sammeln spezieller Anliegen in Bezug auf Gesundheit, Finanzen, Online-Shopping und Standort- und Mobildaten von den Teilnehmenden im Rahmen einer Diskussion.

***Standort- und Mobildaten**

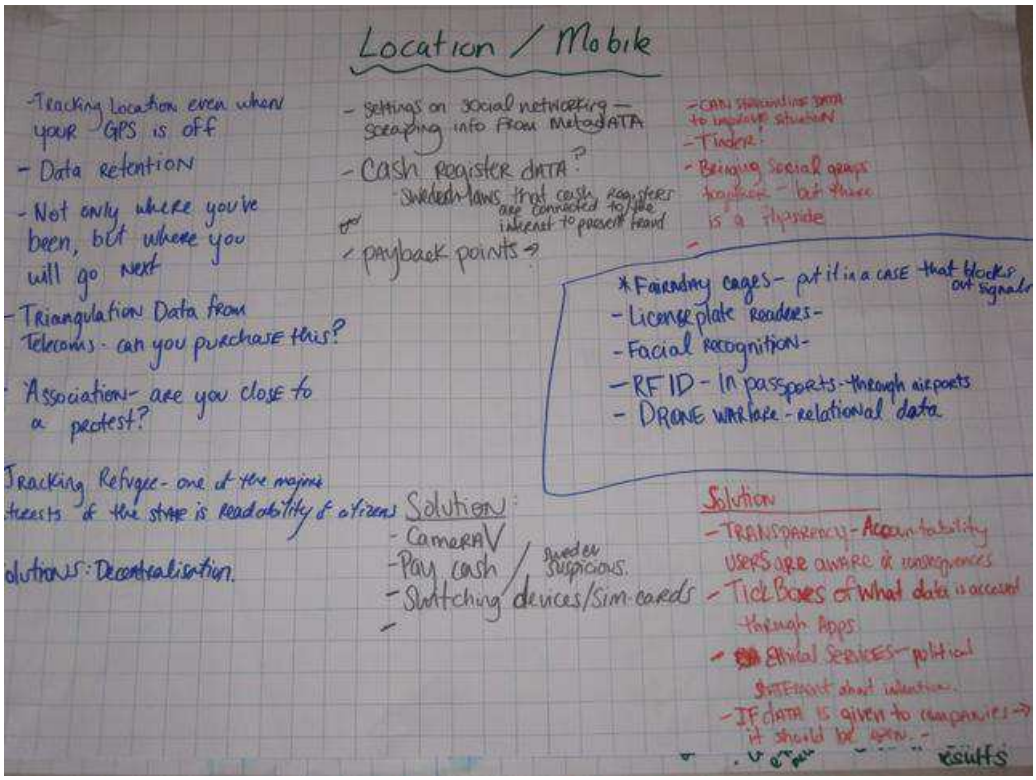
Die meisten Teilnehmenden besaßen ein Smartphone und hatten bereits früher am Tag an der Übung zum Standort-Tracking teilgenommen, bei der gezeigt wurde, welche Standortdaten das iPhone protokolliert. Neben einer Auflistung von Gelegenheiten und Methoden des Standort-Trackings, die die Teilnehmenden für problematisch hielten, ging es ihnen darum, Wege zu finden, das Standort-Tracking zu umgehen. Es wurde festgestellt, dass es nur sehr wenige Möglichkeiten gibt, der Standortverfolgung zu entgehen, wenn man ein Mobiltelefon benutzt. Lösungen wie bspw. faradaysche Käfige sind äußerst unpraktisch und benutzerbezogen, anstatt von der Politik oder Gesetzen gestützt zu werden.

-Alternative Wege, wie unser Standort erfasst wird: wenn man elektronisch bezahlt, Schweden z.B. hat einen hohen Anteil elektronischer Zahlungen, nur wenige benutzen Bargeld. Sobald eine solche Zahlung getätigt wird, werden sowohl der Standort als auch andere Daten protokolliert. In diesem Zusammenhang kann es so außergewöhnlich sein, bar bezahlen zu wollen, dass die Verweigerung der elektronischen Zahlung Verdachte hervorruft. Andere Methoden der Standortbestimmung: Gesichtserkennung, Metadaten in Bildern, Nummernschilderfassung, RFID-Chips in Pässen oder auch Apps wie bspw. Tinder.

- Es gab auch Diskussionsanregungen zu den positiven Aspekten der Standortbestimmung, wobei Plattformen hervorgehoben wurden, die Menschen miteinander verbinden, die sich in derselben Stadt oder Region aufhalten oder etwa GPS-Navigation. Die Runde kam zu dem Schluss, dass diese Technologien und Dienste nützlich sind, aber wir dazu gezwungen werden, unsere Informationen weiterzugeben. Optimalerweise würden wir über Werkzeuge verfügen, bei deren Anwendung die Daten entweder bei uns blieben oder die uns die Möglichkeit gäben, diese nach dem Gebrauch zu löschen (wie etwa GPS-Navigation zu nutzen, ohne dass die Route gespeichert und von Dritten ausgewertet wird).

- Assoziation: auf Basis von Standortdaten werden viele Rückschlüsse gezogen. So ist es z.B. schwierig, zu unterscheiden, ob jemand einen Demonstrationszug photographiert, selbst Demonstrant/in ist oder nur zufällig vorbeigeht, sobald diese Person sich in der Nähe einer Demonstration aufhält.

- Transparenz: Datenschutzrichtlinien sind unklar. Manchmal muss man für die Nutzung einer App große Teile seiner Telefondaten freigeben, ohne dass der Zusammenhang zwischen diesen und dem eigentlichen Dienst ersichtlich ist. Verfügte der Installationsvorgang über Kästchen, mithilfe derer man selbst entscheiden könnte, welche Daten man mit den Diensten zu teilen bereit ist, wäre dies eine deutlich bessere Lösung.

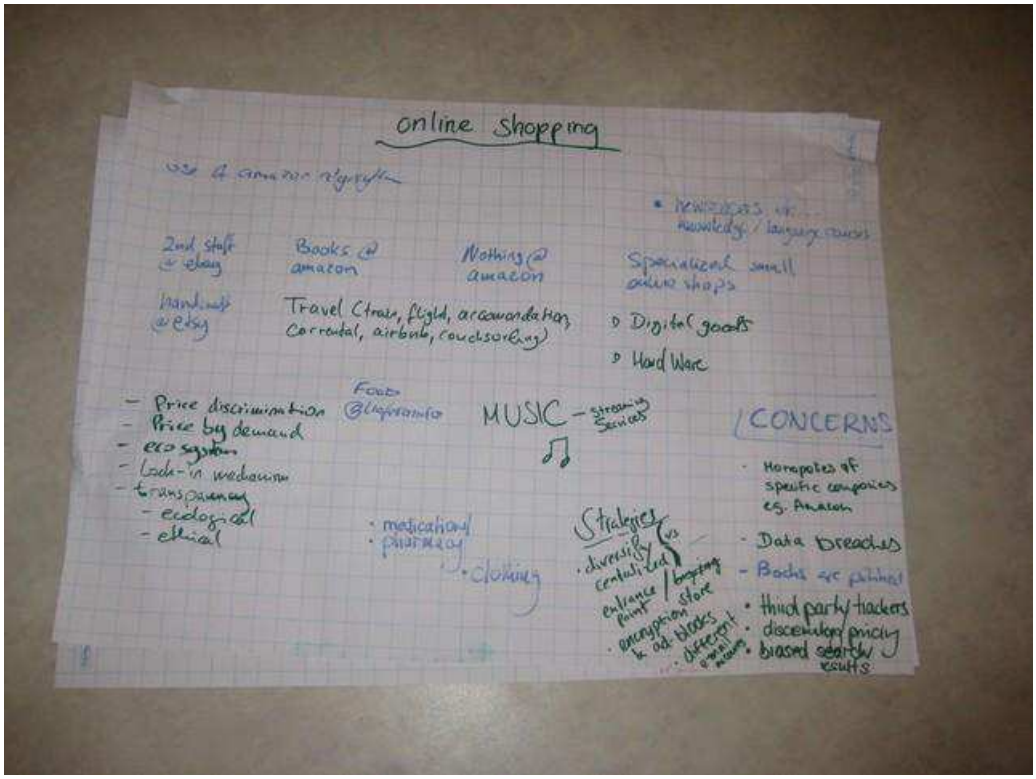


***Online-Shopping**

Es gab große Unterschiede zwischen den Teilnehmenden bei diesem Thema. Einige Leute kaufen beinahe alles online, während andere versuchen, Online-Shopping vollständig zu meiden. Generell wird folgendes meist online gekauft/genutzt: Bücher, Musik, Streaming-Dienste, Reisen (beinahe alle), digitale Güter, Hardware, spezielle Ware und Zeitungsinhalte. Viele hatten gemischte Gefühle und obwohl sie nicht per se gegen Online-Shopping waren, wurden bestimmte Besorgnisse im Zusammenhang mit dem Einkaufen online hervorgebracht. Der vorbestimmende und umstrittenste Akteur im Bereich des Online-Shoppings war für die Teilnehmenden Amazon.

- Probleme wie Preisdiskriminierung, Datenschutzverstöße, auf der eigenen Suche basierende Werbung und welche Muster aus dem eigenen Kaufverhalten abgelesen werden können, wurden artikuliert. So können bspw. Buchkäufe politisch aufgeladen sein, welche Bücher man kauft, sagt vieles über einen aus, z.B. besondere Interessen, bevorzugte Autoren, bevorzugte Schwerpunkte, radikale Literatur etc.

- Lösungen, die hervorgebracht wurden: unterschiedliche Browser und E-Mail-Adressen nutzen, Adblocker einsetzen, Verschlüsselung und/oder Tor benutzen.



***Gesundheit**

Teilnehmende berichteten, dass sie Krankheiten und Symptome recherchieren, sich über Heilmethoden und Medikamente informieren und Foren aufsuchen. Außerdem werden Suchmaschinen genutzt, um Ärzte zu finden.

- DNA-Analyse, Menstruationsmonitore, Smart Watches, Fitness-Tracker, Schlafzyklusmonitore; Gesundheitsdaten sind auf sozialer Ebene besonders persönliche Informationen und daher neigen Verbraucher/innen dazu, bei diesen Dingen sensibler darauf zu reagieren, wenn Daten ohne ihr Einverständnis gesammelt werden oder wenn sie daran denken, dass diese durchsickern und öffentlich gemacht werden könnten.

- Es entbrannte eine rege Diskussion über die Hilflosigkeit bei unklaren Zuständen:
„Daten können Gutes tun, aber auch viel Schaden anrichten, es herrscht keine Transparenz."
„Wo werden die Daten gespeichert und wer kann über sie verfügen?"
„Wir fühlen uns wie Versuchskaninchen, weil viele Informationen ohne unser Wissen angehäuft werden."

-Versicherungen: "Welche Daten werden generiert und was wissen Versicherungen über uns. Wir haben keine Ahnung."

- Gewollter Zugang: „Was wenn ich in verschiedenen Ländern versichert bin - wer hat Zugriff auf diese Daten?“ Die Teilnehmenden erkannten die Vorteile einer zentralen Erfassung in den Fällen an, wenn es Ärzten dabei hilft, mit anderen Ärzten zu kommunizieren, um eine bestmögliche Behandlung gewährleisten zu können (besonders in Fällen von seltenen Krankheiten, bei denen Wissen transferiert und ausgetauscht werden muss).

- Ein immer wieder auftauchendes Thema war der Wunsch nach mehr Transparenz, wobei von der Digitalisierung von Daten im Zusammenhang mit einer Einwilligung der Patienten profitiert werden könnte, wenn diese selbstbestimmten Nutzungsbeschränkungen unterlägen.

- Außerdem gab es eine Diskussion über die Kommerzialisierung der medizinischen Industrie im Zusammenhang mit Datensammlung: Feilbieten von Pharmazeutika und Anzeigen in sozialen Netzwerken, Preisdiskriminierung. Vorurteile: was ist Forschung und was ist Marktforschung? Es wurde als essentiell betrachtet, dass die pharmazeutische Forschung (bspw. an Universitäten) Zugang zu Daten bekommt, wobei Fragen aufkamen, wie der Zugang reguliert werden könnte (Industrie vs. Forschung).

- Verschlüsselung: welche Garantien können uns politische Entscheidungstragende und datensammelnde Einrichtungen bieten? Wenn es neue Kommunikationsmöglichkeiten zwischen Patienten und Ärzten gibt, z.B. via SMS oder E-Mail, sollten auch Methoden zur Verfügung stehen, diese sicherer und vertraulicher zu gestalten.

***Finanzdaten**

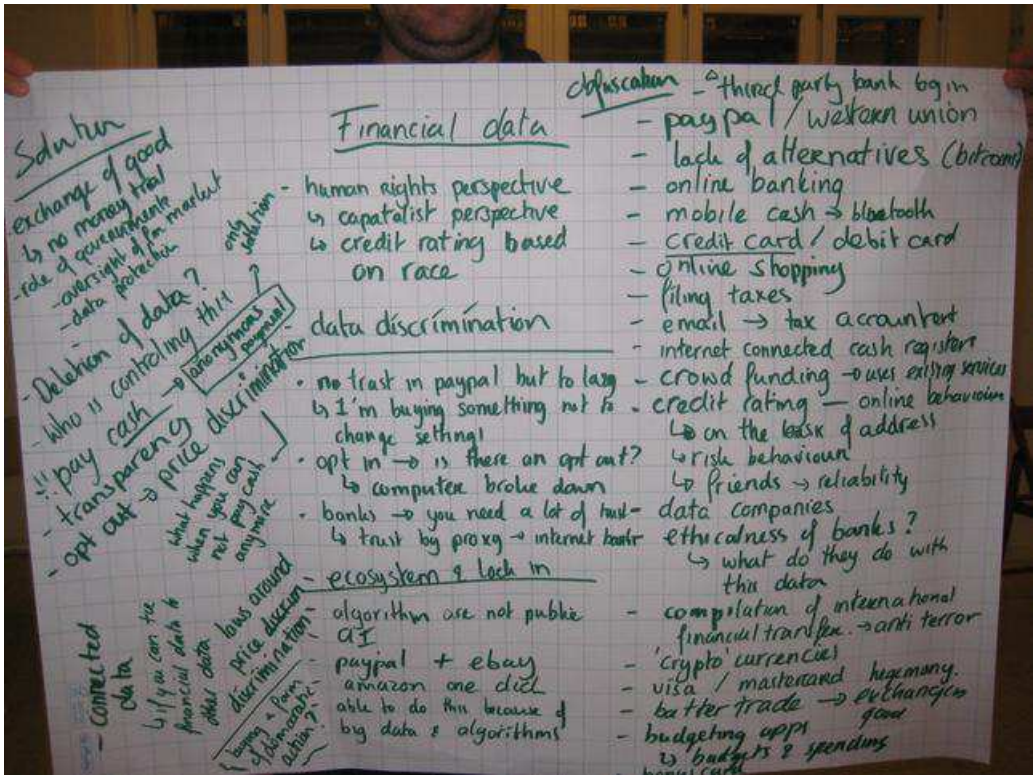
- Bürgerinnen und Bürger übertragen Finanzinformationen durch alltägliche Interaktionen wie Online-Banking, die Nutzung von Kredit- und EC-Karten, Steuererklärungen, Budgetierungs-Apps, mobile Zahlungsverfahren und Online-Shopping.

- Angesprochene Probleme drehten sich vor allem um Datenerhebungen und Diskriminierung durch Bonitätsbewertungen und den Mangel an Alternativen. Die Teilnehmenden fanden es merkwürdig, dass wir keinen Zugriff darauf haben, welche Daten in Bonitäts- und Kreditbewertungen einfließen. Andere erwähnten, dass sie PayPal nicht vertrauen würden, vor allem jetzt, wo es ein Teil von eBay ist, ihnen aber die Zeit oder Energie fehlte, all diese Einstellungen manuell zu verändern, damit die beiden nicht mehr direkt miteinander kommunizieren.

- Darüber hinaus kritisierten die Teilnehmenden den Mangel an Alternativen und bezeichneten die Bindung an bestimmte Systeme als frustrierend.

- Transparenz: wenn Algorithmen proprietär aufgebaut sind, wie soll man sie dann ihre Funktionen und potentielle Gefahren evaluieren?

- Mögliche Lösungsansätze wurden hervorgebracht: bar zahlen und das schwedische Modell einer bargeldlosen Gesellschaft meiden, da Bargeld die einzige „anonyme“ Währung wäre. Die Regierung sollte die Aufsicht auf dem Finanzsektor auch über Banken hinaus haben, z.B. wenn es um Zahlungspläne, Kredit-Ratings oder mobile Zahlungsmethoden geht. Es sollte transparenter sein, welche Verbindungen zwischen Unternehmen bestehen und außerdem sollte es eine Möglichkeit geben, einzusehen, ob man selbst „diskriminiert“ wird.



15:45-16:30 *Rekapitulation*

Durchführung: Die Teilnehmenden wurden angehalten, eine zusammenfassende Empfehlung oder eine Forderung auszusprechen, die ihrer Meinung nach die momentane Situation verbessern könnte in Bezug auf die aktuelle Politik oder im Zusammenhang mit einem neuen Produkt oder einer Software.

Ziel: Diese Übung sollte es den Teilnehmenden ermöglichen, eine direkte Empfehlung zu formulieren, nachdem sie den Tag über viele Facetten des Datenschattens diskutiert hatten. Damit wurden ihre Meinungen und Verbesserungsvorschläge zusammenfassend vorgetragen.

Direkte Handlungsempfehlungen an die Politik im Bereich des Verbraucherschutzes haben wir kursiv gesetzt:

Verbraucher/innenwahrnehmung

- Transparenz: was geschieht mit meinen Daten, wo landen sie?
- Das Bewusstsein, dass wir nicht immer zustimmen müssen. Nicht jedes Feld muss ausgefüllt und mit Informationen bezahlt werden
- Crypto-Partys, vor allem zum Community-Building
- *Mehr Bildung und Informationen: Technologien entwickeln sich schneller fort als unsere Rechts- und Bildungssysteme, weshalb viele Bürger und Bürgerinnen unzureichend über die Möglichkeiten und Abläufe der massenhaften Datenspeicherung informiert sind. Ein kleingedruckter Abschnitt in den Nutzungsbedingungen als einzige Information reicht nicht aus. Wir benötigen mehr Programme und Workshops wie diesen an Schulen, in Betrieben usw.*

Technische Lösungsansätze

- Dem User sollten mehr Möglichkeiten übertragen, mehr Kontrolle gegeben werden
- Freiheitliche Cloud und lokale Datenspeicherung. „Ich würde Geld dafür bezahlen, wenn man mir garantiert, dass meine Daten nicht verkauft werden."
- Förderung und Unterstützung dezentralisierter Plattformen

Politische Lösungsansätze

- *Nutzungsbestimmungen kürzer und klarer gestalten*
- *Haftung: wer übernimmt die Verantwortung bei einem Datenleck? Werden wir entschädigt, wenn unsere persönlichen Informationen durchsickern und damit zum Risikofaktor werden können? Gibt es Abschreckungsmittel gegen Firmen, unsere Daten zu sammeln oder besser Anreize, die Menge gesammelter Daten und die Dauer der Speicherung zu beschränken?*
- *Datenschutzzertifikate/-siegel: ähnlich wie Energiesiegel bei Glühbirnen*

- *Mehr Bildung und Informationen: Datenkompetenz sollte ein Teil des Bildungssystems sein*
- *Der Staat sollte eine Vorbildfunktion für Open-Source-Systeme übernehmen, diese sind günstiger und sicherer.*
- *Es muss davon ausgegangen werden, dass Firmen Datensicherheits-bestimmungen zu ihrem Vorteil nutzen. Man muss bei der Gesetzgebung vom schlimmsten Fall ausgehen, weil wir immer wieder aufs Neue beobachten, dass Firmen, vor allem auf dem Sektor der Neuen Technologien, Wege finden, die Grenzen des Machbaren neu zu definieren, meistens auf Kosten der Allgemeinheit.*
- *Ablaufdatum für Daten: wobei Daten, unerheblich ob sie personifiziert oder anonym sind, ein Ablaufdatum erhalten und anschließend unwiderruflich gelöscht werden.*

Fragen und Kommentare

- *Wir sollten in der Lage sein, unseren Datenschatten einzusehen, genauso wie wir unsere Bonitätseinstufung abrufen können. Welche Annahmen machen Firmen auf Basis unserer Daten?*
- Sollten alle Daten „offen“ sein (anonymisiert)? All diese Informationen sollten sich nicht in den Händen weniger befinden. Vor allem, wenn es von vornherein über unsere eigenen Daten als Bürger geht.
- *Wird Datenschutz zu einem Privileg der Eliten? Dies wäre für eine faire und gesunde Gesellschaftsordnung äußerst hinderlich, scheint aber die Richtung zu sein, in die es sich bewegt.*
- Datenschutz sollte nicht nur ein Argument im Zusammenhang mit Überwachung und Privatsphäre sein – er verbindet viele Themen aus anderen Bereichen miteinander und sollte stärker in den Mittelpunkt gerückt werden.

Fazit und Analyse

Im Laufe des Tages kam es zu einer Verschiebung der Wahrnehmungen und damit auch der geäußerten Sorgen. Die Empfindung der Teilnehmenden in Bezug auf Daten und Datensicherheit wandelte sich im Laufe des Workshops von Neugier zu einer Gruppe von Leuten, sie sich besser darüber informiert sah, was tatsächlich geschieht. Einige Kommentare am Ende des Workshops drehten sich darum, dass viele Fälle von Datensammlung hinter geschlossenen Türen stattfinden und Verbraucher/innen besser aufgeklärt werden und Regierungen Sorge tragen sollten, die Bildung und Wahrnehmung zu diesen Fragen zu erhöhen.

Darüber hinaus tauchten einige Anliegen immer wieder auf, die sich um eine Abkehr vom aktuellen Status Quo drehten. Diese beinhalteten Aufrufe, Firmen stärker zu regulieren und sie zu verpflichten, ihre Sicherheitsbestimmungen transparenter zu gestalten und den Verbraucher/innen die Möglichkeit zu liefern, ihre eigenen Daten besser kontrollieren zu können.

Wir haben außerdem festgestellt, dass die Teilnehmenden an praktischen, selbstbestimmten Lösungen interessiert waren, also z.B. dem Herunterladen bestimmter Add-Ons, der Nutzung sicherer Browser oder gar einer Veränderung der eigenen Gewohnheiten, indem Telefone ausgeschaltet oder die Akkus entfernt werden, sobald das Telefon nicht im Betrieb ist, um der Protokollierung der eigenen Bewegungen und Aktivitäten zu entgehen. Dies könnte an der Ausrichtung des Workshops durch Tactical Tech liegen oder aber Verbraucher/innen bewerten es als schwierig, direkte Empfehlungen an die Politik oder Verbraucherschutzorganisationen auszusprechen, wie die Datensicherheit erhöht werden könnte. Vielleicht auch, wie bereits erwähnt wurde, weil die Politik und Gesetze oft den eigentlichen technologischen Entwicklungen weit hinterherhinken.

Damit lässt sich zusammenfassend sagen, dass die Teilnehmenden in der Lage waren, ihre Anliegen in Bezug auf eine große Bandbreite von Themen zu artikulieren und gleichzeitig erstaunliche Lösungsvorschläge hervorgebracht haben, von denen viele allerdings nur auf der politischen und gesetzlichen Ebene implementiert werden können. Wir hoffen, dass diese mit der notwendigen Offenheit rezipiert werden und für zukünftige Verbraucherschutz-maßnahmen in der digitalen Sphäre zu Rate gezogen werden.

Anhang 1: Post-it-Dokumentierung

Cluster: Companies
- State and commerce come together
- Data shared by third parties
- Economic / commercial surveillance
- Evil companies work together to manipulate me... in what ever capacity
- Customized advertising
- State - industrial complex

Cluster: Technical
- Connection and weighing between data protection and anti discrimination law
- Data protection norms / legal
- Identification and tracking technologies via multiple devices and account
- Trade-off Balance e.g. Good Cookies vs Bad Cookies
- Technology behind traces
- Trust and data services, consumer protection
- What about these custom password programs, if they get hacked then obviously you are worse off then someone finding your normal password
- Is it possible to 'edit' my Google trail?
- Data islands (independent clusters)
- Magic = control
- Effective privacy tools
- Can we live a normal life offline in 5,10 or 15 years?
- Practical means to protect personal data
- How to limit what others' data can tell about you
- Data ownership
- Creating and building community network maps showing social relations
- Risk prognosis
- Digital shadows used during recruitment process
- Psychological reasoning
- Who is the object of persuasive technologies?
- Reputation
- Who wants the data?
- Empirical studies about Data Deletion Demands by Consumers
- Many unknowns: Fear out of not knowing what to fear
- Why is it crucial to give my phone number to recover my email

Cluster:Surveillance
- Surveillance as the internet business model
- Data / Digital world: how is the curricular education system altering?
- Surveillance
- "Sousveillance" is down, distributed counter surveillance is up.
- Interlinked data (cross platform)
- Issues / Cases about identity theft
- Identity theft
- eHealth and self-surveillance
- Comparison of ToC and Privacy Policies over time, companies and countries
- Security of Mobile Apps
- What is my data shadow, when I play via App?

Cluster: curation
- Functional sets (combis)

- Are there alternative ways to collect data?
- Information as new material (Accordances?)
- How to make shadows visible
- Digital shadows imaginary (Peter Pan?)
- How can I "curate" my digital shadow? To what extent?

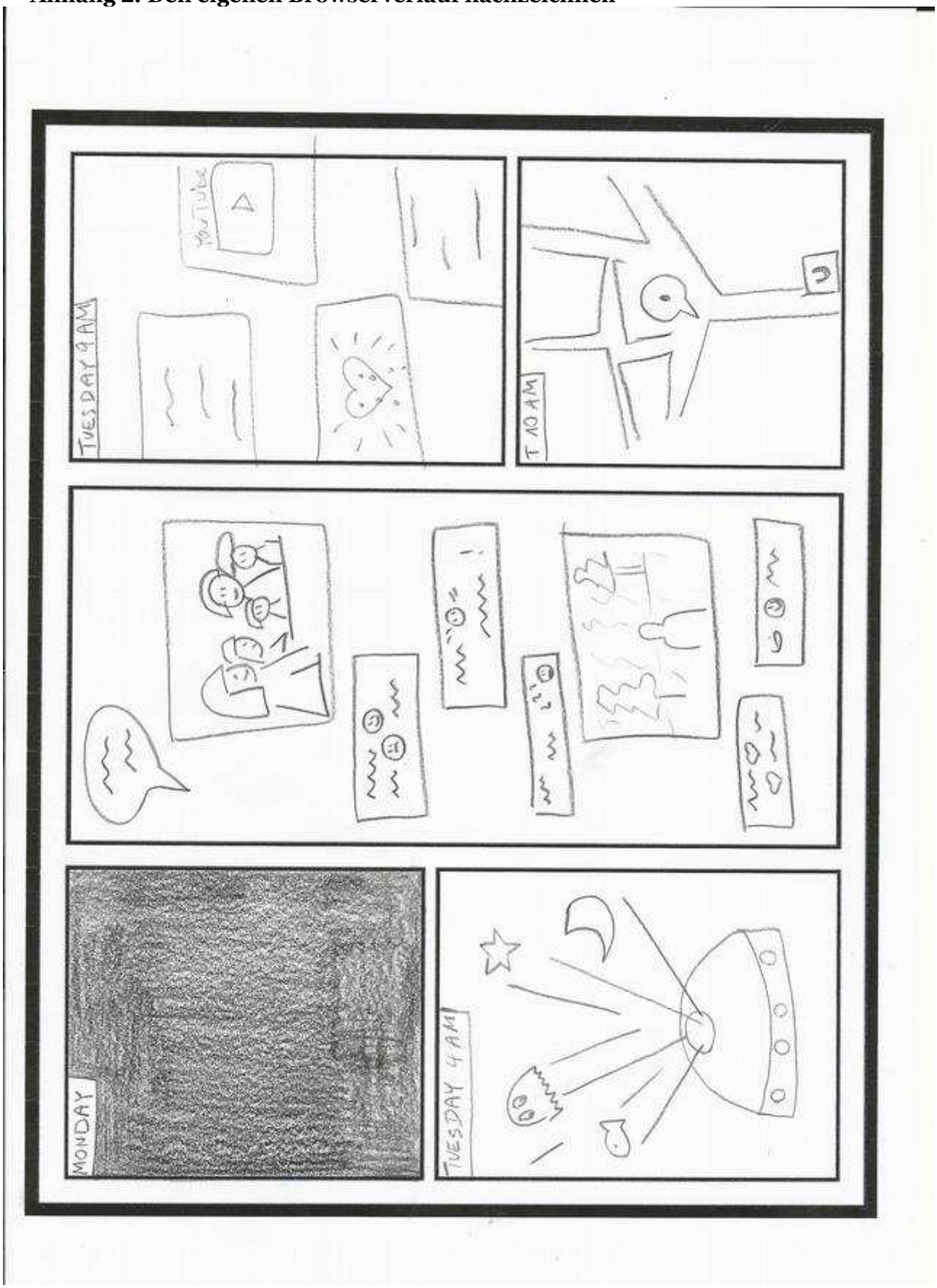
Cluster:Interconnectedness
- How to set up a privacy sensible data collection infrastructure
- Operationalization of human activities (profiles)
- Re-purposing data
- What's the price of my shadow?
- Connection between different mail accounts
- Mix ups: ending up on a no-fly list b/c someone messed up data
- Visibility (for whom), connection between mobile apps and social media i.e games and Facebook
- Retro policing
- Unique personal identifier
- Predictable people
- What does Google know when I'm logged into my Gmail account and I open / visit different websites?
- Is my Posteo mail account "safer" when I'm surfing parallel and other websites?

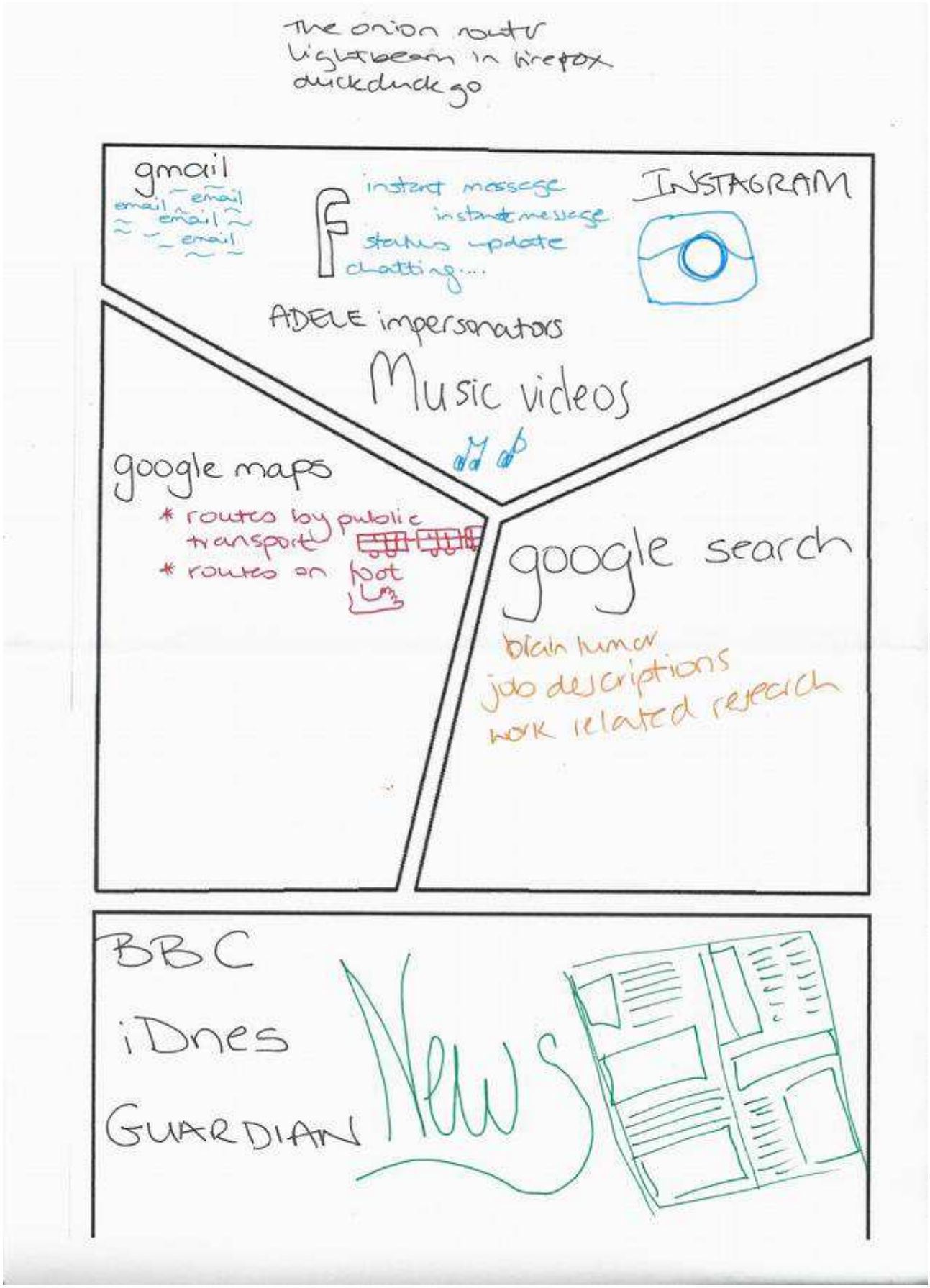
Cluster: Social
- How to reach common people about surveillance? Education? PR? Lobby?
- What happens if something hacked my email account?
- Social etiquette
- What is actual accessibility to my FB profile for my non friends?
- What effect will going dark in social media have for me?
- How to allow also craft makers to create shadows
- Erasing data
- Where does info go when I delete it aka emails but also profile info etc?
- How explain online privacy to kids
- When you delete an account (Facebook, Pinterest, Twitter, Instagram etc.) does it really disappear?
- It is true, that people can look up my Chronic if they know my ID (computer ID)?
- Online privacy as shared social responsibility
- How to intentionally shape the shadow?
- Location
- Mapping location of people: past, present and possible future

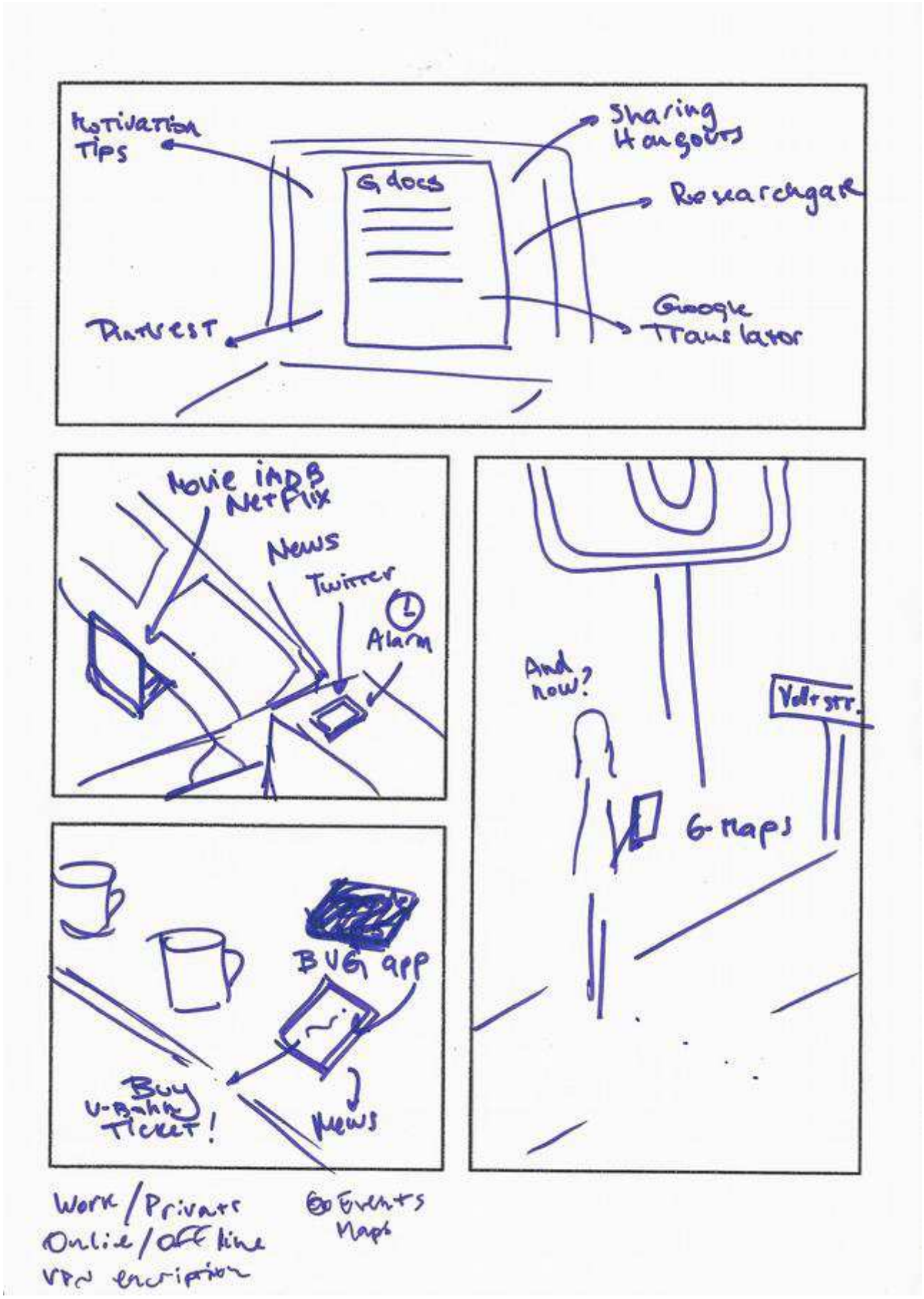
Cluster: Ethics:
- Loss of control over my data, apps that can track me without my consent (for other users)
- Economic and data
- Subversion, persecution of encryption
- What kind of data is used for what?
- Data and my relationships
- Ethics of surveillance and privacy
- Global Digital Flows
- Not leaving traces (strategies?)
- Targeting of political activists
- Social justice through race and equality data
- Safe places to communicate your opinion under real name?

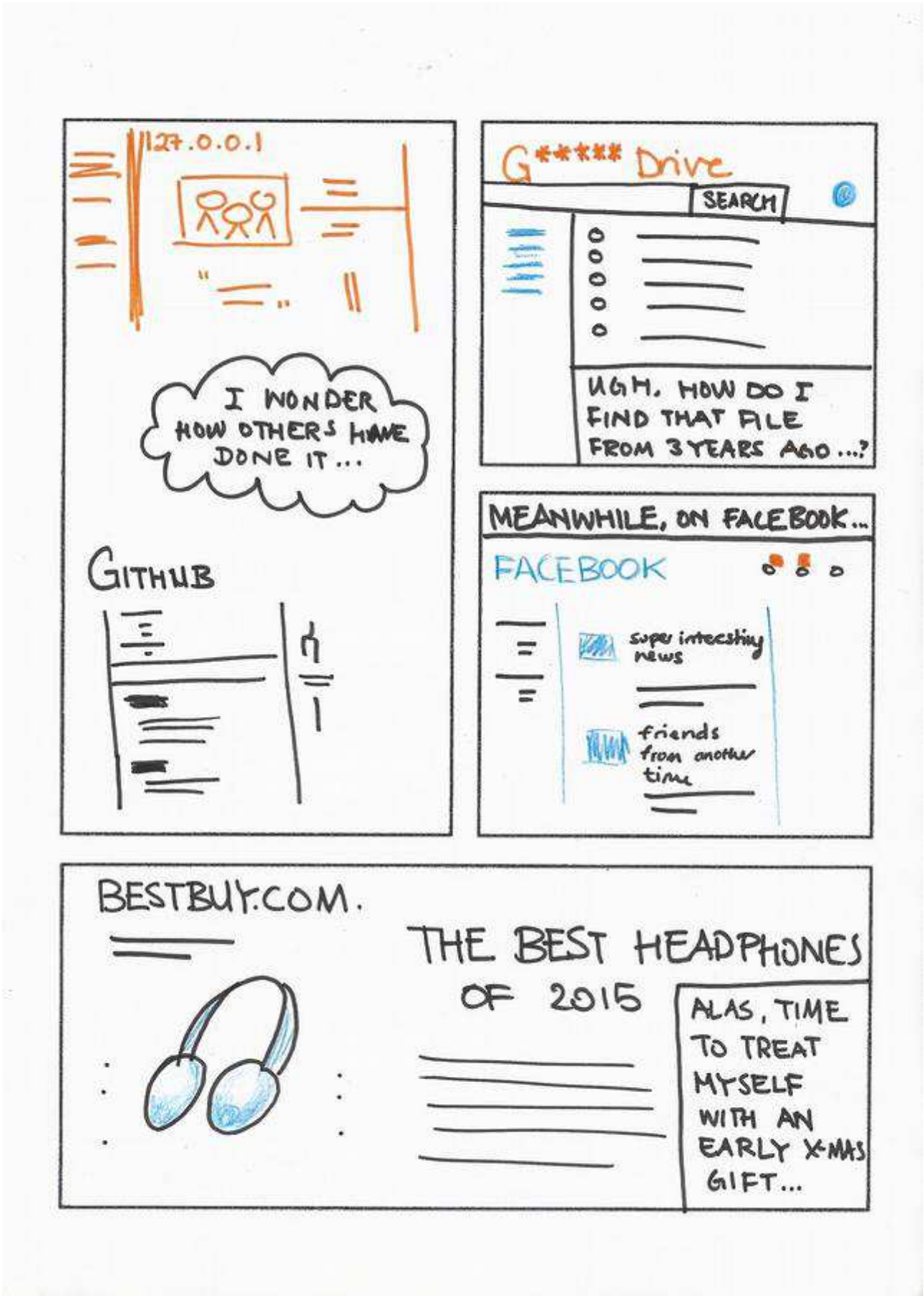
- Is there anything positive that comes out of large data collection? (ie. political views being collected and acting as a new form of democracy
- Data exchange between companies
- Data and consent
- How to protect ourself?
- Ethics in social research related to data protection?
- My shadow knows what I know
- Opt out vs Opt in

Anhang 2: Den eigenen Browserverlauf nachzeichnen




The onion router
lightbeam in firefox
duckduckgo
gmail
email
email
email
email
F
instant message
instant message
status update
chatting....
INSTAGRAM
ADELE impersonators
Music videos
google maps
* routes by public transport
* routes on foot
google search
brain tumor
job descriptions
work related research
BBC
iDnes
GUARDIAN
News


Motivation Tips
Sharing Hangouts
G docs
Researchgate
Pinterest
Google Translator
Movie IMDB Netflix
News
Twitter
Alarm
And now?
Volkstr.
G-maps
BVG app
Buy U-Bahn Ticket!
News
Work / Private
Online / Offline
VPN encription
Events
Maps


127.0.0.1
I WONDER HOW OTHERS HAVE DONE IT...
GITHUB
G***** Drive
SEARCH
UGH. HOW DO I FIND THAT FILE FROM 3 YEARS AGO...?
MEANWHILE, ON FACEBOOK...
FACEBOOK
super interesting news
friends from another time
BESTBUY.COM.
THE BEST HEADPHONES OF 2015
ALAS, TIME TO TREAT MYSELF WITH AN EARLY X-MAS GIFT...

Anhang 3: Handlungsempfehlungen an die Politik (Abschlussrunde)

- Some sort of transparency- what happens to my data, where does it end up- including a visualisation of the movements
- Freedom-box- local data storage gives the user autonomy
- Awareness of possibilities- we don't always have to opt-in or fill in every box, but there are few mechanisms to raise awareness about this and other digital literacy practices
- Crypto parties- especially as a form of community building
- Don't put these issues into a box of privacy and surveillance issues- they relate to many other areas and need to be connected to them for people to engage in the topic
- Data sovereignty
- Shorten and clarify terms of services
- Accountability! who is taking responsibility for what happens to our data- is there any incentives for companies to think twice about this? to think about the cost of our personal information being leaked?
- What kind of data is being collected? We as citizens should know this, and we should be able to request to see the "shadow" that has been created for us, just as we can see our credit ratings
- Freedom-Box- I would pay money for services that ensure that they don't sell my data.
- Decentralised platforms
- Certification for privacy- similar to energy ratings that come on every light bulb
- More education and information. there is not literacy or awareness raising in our educations systems. Technology is moving faster than our legal and education systems.
- The state should be a role model for open source. It's more secure and less expensive
- More open data (when it is anonimised). all of this information should not be in the hands of few.
- When data protection laws are written assume that corporations will take as much advantage of it as possible. Assume the worst case scenario and make laws strong enough to prevent them from being taken advantage of.
- Will privacy be something for the privileged? this should obviously not be so for a healthy and fair civil society.
- An expiration date on data stored

Sachverständigenrat für Verbraucherfragen

Der Sachverständigenrat für Verbraucherfragen ist ein Beratungsgremium des Bundesministeriums der Justiz und für Verbraucherschutz (BMJV). Er wurde im November 2014 vom Bundesminister der Justiz und für Verbraucherschutz, Heiko Maas, eingerichtet. Der Sachverständigenrat für Verbraucherfragen soll auf der Basis wissenschaftlicher Erkenntnisse und unter Berücksichtigung der Erfahrungen aus der Praxis das Bundesministerium der Justiz und für Verbraucherschutz bei der Gestaltung der Verbraucherpolitik unterstützen.

Der Sachverständigenrat ist unabhängig und hat seinen Sitz in Berlin.

Vorsitzende des Sachverständigenrats ist Prof. Dr. Lucia Reisch.

SVRV Sachverständigenrat für Verbraucherfragen