Was hat Überwachung mit Sex und Gender zu tun?

Shephard, Nicole

2017

https://doi.org/10.25595/1384

Veröffentlichungsversion / published version

Sammelbandbeitrag / collection article

Empfohlene Zitierung / Suggested Citation:
Shephard, Nicole: *Was hat Überwachung mit Sex und Gender zu tun?*, in: Baumann, Hans; Gallusser, Martin; Herzog, Roland; Klotz, Ute; Michel, Christine; Ringger, Beat; Schatz, Holger (Hrsg.): Technisierte Gesellschaft : Bestandsaufnahmen und kritische Analyse eines Hypes (Zürich: edition 8, 2017), 108-116. DOI: https://doi.org/10.25595/1384.

Was hat Überwachung mit Sex und Gender zu tun?

Es war einmal ein kleiner Vibrator, der wollte gerne nach Hause telefonieren. An der DEFCON-Konferenz 2016 wurde gezeigt[1], dass der We-Vibe 4 Plus genau dies regelmässig tat. Ohne Wissen der zwei Millionen BenutzerInnen schickte das Gerät Daten zu Intensität, Modus, und Körpertemperatur an den Hersteller Standard Innovation, wo sie – mit Zeitstempel und E-Mail-Adressen versehen – gespeichert wurden.[2] Selten ist der Zusammenhang zwischen Überwachung und Sexualität so offensichtlich. Dieser Beitrag widmet sich deshalb der Schnittstelle zwischen Big Data, Überwachung und feministischer Theorie aus intersektioneller[3] Perspektive.

Voraussetzung ist dabei das Grundverständnis, dass Daten, wie auch ihre Verarbeitung und Auswertung, keineswegs einfach objektiv und neutral sind (Gitelman 2013). Im Gegenteil, alle Methoden der Datensammlung und -analyse sind Rahmenbedingungen unterworfen, unterliegen Annahmen und Ausschlüssen, werden eher im globalen Norden initIert als anderswo und werden signifikant häufiger von jemandem aus der Kategorie Weiss, Männlich, und Heterosexuell durchgeführt als von allen anderen. Daten, auch Big Data, sind ausserdem stets eine Stichprobe, keine Population (Kitchin 2014). Auch sogenannte Metadaten sind von dieser Logik nicht ausgenommen, denn sie erlauben Rückschlüsse auf Verhalten, Beziehungen, Vorlieben und Identität, die gar tiefer greifen können als der eigentliche Inhalt einer Mitteilung (UN OHCHR 2014).

Dataveillance (Raley 2013) ist ein prägnantes Kompositum aus Daten und Überwachung und erfasst eine konzeptionelle Verschiebung von einer beschreibenden Datenpraxis hin zu datenbasierter Vorhersage und normativer Verschreibung. Staatliche Massenüberwachung, oft formuliert als Patentrezept der nationalen Sicherheit, steht im Vordergrund des öffentlichen Diskurses. Dataveillance umfasst aber auch die kommerzielle Überwachung und individualisierte Formen lateraler Überwachung (Andrejevic 2005); in der freien Wildbahn treten diese Ebenen jedoch meist verschränkt auf. Schliesslich beliefern

Nicole Shepard

ist promovierte freie Sozialwissenschaftlerin und Autorin. Sie beschäftigt sich mit den Schnittstellen zwischen Queer/Feministischer Theorie und den Technologien, die unsere vernetzten Gesellschaften zunehmend prägen.

zum Beispiel Daten der sozialen Medien in erster Linie das personalisierte Werbegeschäft, dienen aber gleichzeitig als Schauplatz lateraler Überwachung. Aufgrund der gängigen ›Collect it all‹-Logik staatlicher Akteure geraten dieselben Daten letztlich auch in die Fänge staatlicher Massenüberwachung, wie wir spätestens seit Edward Snowden wissen.

Der Vibrator-Hersteller Standard Innovation erklärte sich im Rahmen eines aussergerichtlichen Vergleichs bereit, die fraglichen Daten zu löschen und keine weiteren zu sammeln (Freytas-Tamuramarch 2017). Nachrichten über Sicherheitslücken und Datenpannen im ›Internet of Things‹ sind aber an der Tagesordnung. Was mit den Intimdaten der BenutzerInnen ohne DEFCON-Vortrag und anschliessende Sammelklage längerfristig passiert wäre, bleibt in diesem Falle Spekulation.

Kontinuitäten

Daten sind bereits zu prä-digitaler Zeit fleissig gesammelt worden: Ganze wissenschaftliche Disziplinen und bürokratische Apparate dienten der Kontrolle von Bevölkerungen, Kolonien, Imperien und der gewaltsamen Durchsetzung deren institutioneller Ordnung. Dass Gender, Sexualität und ›Rasse‹ dabei eine tragende Rolle spielten, ist bestens belegt (Stoler 2010; McClintock 1995).

Der Körper und die Teilhabe von Frauen, von SklavInnen, ArbeiterInnen, MigrantInnen, von Kranken oder Armen, standen seit jeher unter staatlicher und gesellschaftlicher Überwachung. Überwachungsstudien feministischer, postkolonialer und antirassistischer Ausprägung weisen auf Kontinuitäten zwischen Online- und Offline-Diskriminierung, aber auch zwischen alten und neuen Formen der Überwachung hin. Obwohl stets bestrebt, alles zu sehen und zu erfassen, geht es der Überwachung mitunter auch darum, ihr hetero-patriarchales Kolonialerbe *nicht* zu sehen (Smith 2015).

Simone Browne (2015) beschreibt die rassifizierte Überwachung unter anderem als eine Technologie der sozialen Kontrolle, welche alte Normen (re-)produziert und bestimmt, wer ›in or out of place‹ ist, also wer wo (un)erwünscht ist. Auf den Spuren von Überwachungstechnologien des transatlantischen Sklavenhandels zeigt sie auf, dass diese Normen sowohl in der heutigen Überwachungspraxis nachhallen als auch im Diskurs und in der Forschung zu Überwachung relevant bleiben. Hat man sich das erst zu Gemüte geführt, fällt es schwer, keine Zusammenhänge zwischen vergangenen Praktiken körperlicher Vermessung oder der Brandmarkung von Sklaven und der heutigen biometrischen Datenerfassung oder der Gesichtserkennungstechnologie zu sehen. Auch das inzwischen omnipräsente Racial Profiling – besonders von MuslimIn-

nen – an Landesgrenzen und auf der Strasse wäre post-9/11 kaum denkbar geworden ohne die kolonialen, orientalistischen und rassistischen Logiken, die es ermöglichen.

Dataveillance ist so gesehen also höchstens die neueste Ausprägung eines abendländischen Taxonomie-Fetischs mit langer, dunkler Geschichte. In Anbetracht der rasanten Entwicklungen im Bereich von Big Data sowie des Ausbaus der staatlichen und kommerziellen Überwachungspraxis bleibt es aber angezeigt, sich neben Technik und Recht auch mit den sozialen und kulturellen Auswirkungen auseinanderzusetzen. Ehemals getrennte Lebensbereiche konvergieren inzwischen in Daten: Soziale Beziehungen, Arbeit, Konsum, Kommunikation, Unterhaltung und Bildung, aber auch Gesundheit, Finanzen und staatliche Sozialleistungen hinterlassen immer mehr Datenspuren. Zwar wird diese Entwicklung zugleich zelebriert und problematisiert, doch kommen ihre intersektionellen Implikationen im öffentlichen Diskurs zu kurz.

Überwachte(r) Körper

Dass die Trennung zwischen digitalem und realem Leben nicht standhält, sondern beide verschränkt und durchaus echt sind, ist inzwischen fast Allgemeingut. Wenn Menschen zu Datenpunkten werden, erfolgt eine Informatisierung des Körpers, die eine eindeutige Trennung zwischen dem Körper *an sich* und seiner digitalen Repräsentation infrage stellt (van der Ploeg 2003). Körper sind auch durch Produktion und Konsum in Datenpraktiken eingebunden, woraus sich neue Normativitäten zur eigenen Körper- und Datenpraxis ergeben können. Der Körper *als Daten* geht einher mit vielerlei Methoden, ihn zu überwachen und zu kategorisieren (van der Ploeg 2012).

Betrachtet man Überwachung intersektionell, tritt der Körper denn auch als wichtiger Austragungspunkt auf (Monahan 2009). Überwachungstechnologien sind oft nicht auf alle Körper gleichermassen zugeschnitten, sondern privilegieren weisse Männerkörper ohne Behinderung. Was passiert, wenn Körper ausserhalb dieser impliziten Norm auf solche Technologien treffen, illustriert den Bedarf an intersektionellen Überwachungsstudien. Bekannte Beispiele sind Ganzkörperscanner in Flughäfen, die genderqueere oder behinderte Menschen überproportional herausgreifen (Magnet/Rodgers 2012); Google-Suchresultate, die mehrheitlich schwarze Frauen mit natürlichem Haar als Suchresultat für ›unprofessional hair‹ produzieren, aber mehrheitlich konventionell attraktive weisse Menschen für ›men‹ oder ›women‹ (Alexander 2016); oder auch die Geschichte des Farbfilms, der noch nicht lange in der Lage ist, auch dunkle Hauttöne in guter Qualität abzubilden.[4]

›Othered bodies‹, anders konstruierte Körper, unterliegen erhöhter Überwachung und werden als suspekt aussortiert und (noch) eingehender überwacht. Von diesem Mechanismus besonders betroffen sind Körper an den Schnittstellen der Differenzierungen zwischen »transgendered, disabled, fat, religious, female and racialized« (Magnet/Rodgers 2012). Magnet beschreibt z.B., wie biometrische Technologien am häufigsten an Frauen, an nicht-weissen Menschen, an behinderten Menschen und an anderen körperlichen Abweichungen scheitern (Magnet 2011). Das ist besonders problematisch, weil biometrische Technologien auch zur staatlichen Kontrolle, etwa von Geflüchteten oder EmpfängerInnen sozialstaatlicher Leistungen, oder an Landesgrenzen eingesetzt werden.

Etwas anders geartet sei hier auch der Trend zur Selbstquantifizierung erwähnt, wo die fliessenden Grenzen zwischen kommerzieller und lateraler Überwachung zusätzlich mit Selbstüberwachung verschmelzen. Das Erfassen, Tracken und Teilen von Daten zu Gesundheit, Fitness, Ernährung oder sportlicher Betätigung wird zunehmend ergänzt durch Daten zur reproduktiven Gesundheit, zum Beispiel zu Menstruation, Schwangerschaft und Fruchtbarkeit. Daten entstehen dabei durch die manuelle Erfassung von Zyklen und Symptomen, aber auch aus Messungen von Körper- und Vaginaltemperatur oder Blutwerten durch appspezifische Hardware. Das kann einerseits als positive Entwicklung gewertet werden; schliesslich machen Frauen die Hälfte der Bevölkerung aus und haben gesundheitlich spezifische Anliegen, die in Daten wie auch anderswo oft zu kurz kommen. Aber: »Data from millions of women who are using these apps are used to develop a ›normal‹ standard of healthy female cycles, drawing on the data of the users – mostly American and European white women. This leads to the significant question of what this mass quantification of women's bodies means for the creation of new normals, of new standards for reproductive and gynecological indicators based only on those women who have access to these apps, and those who bother to use them« (Rizk/Othman 2016).

Was als teilweise Ausgleichung einer einseitigen Datenlage anmutet, muss also vorsichtig bewertet werden. Wie so oft entstehen Daten im globalen Norden, werden weisse Körper zur Norm erhoben. Ausserdem entstehen durch Selbstquantifizierung Datensätze über Frauenkörper, die nicht nur mit der app-eigenen Plattform, sondern auch mit unbekannten Dritten geteilt werden und primär der kommerziellen Überwachung dienen. Neben allgemeinen Fragen zur Datensicherheit entstehen dabei Implikationen für gesellschaftliche Körper- und Gesundheitsbilder, aber auch in Bezug auf Privatsphäre und Selbstbestimmung – schliesslich stellen Intimdaten den Extremfall persönlicher Daten dar.

Algorithmische Diskriminierung

Hier geht es nicht in erster Linie darum, EntwicklerInnen rassistische, sexistische, homo-, oder transphobe *Absichten* zu unterstellen. Vielmehr können Technologien diskriminierende *Auswirkungen* haben, wie sich in der Praxis immer wieder zeigt. Man erinnere sich etwa an TAY, Microsofts niedlich gedachten KI-Chatbot: Kaum einen Tag den rassistischen und sexistischen Eskapaden der twitternden Öffentlichkeit ausgesetzt, ging TAY offline, weil es sich durch Machine-Learning-Algorithmen vom hippen Teenager zu einem ›Hitler-loving sex robot‹ entwickelte (Horton 2016).

TAY mag ein Extrembeispiel sein und als medienwirksames PR-Desaster sogar komisch anmuten. Dass Machine-Learning-Algorithmen gesellschaftliche Vorurteile reproduzieren, ist hingegen wissenschaftlich belegt (Caliskan et al. 2017) und äusserst ernst zu nehmen. Wenn die öffentliche Verwaltung, die Strafverfolgung, das Gesundheitswesen, die internationale Zusammenarbeit, die nationale Sicherheit wie auch viele Sektoren der Privatwirtschaft Big Data vermehrt in ihre Praxis aufnehmen, verschwimmen nicht nur die Grenzen zwischen Administration und Überwachung; Rassismus, Sexismus und andere historisch, gesellschaftlich und kulturell tief verankerte Diskriminierungen reproduzieren sich auch algorithmisch. Vorhersagemodelle zielen zwar auf künftige Ereignisse, beziehen sich aber zwangsläufig auf Daten und Zusammenhänge der Vergangenheit. So lernen sie bestehende Muster und Diskriminierungen zu reproduzieren statt aus ihnen zu lernen.

Statistische und algorithmische Methoden beruhen ausserdem definitionsgemäss auf einer Proximität zur Norm; und meist ist die implizite Norm, an der alle Datenkörper gemessen werden, weiss, männlich, cisgender und heterosexuell. Abweichungen werden kaum berücksichtigt, womit es an Raum fehlt, um dem Rauschen, der Mutation oder subversiver Störung gerecht zu werden (Conrad 2009). Besonders sichtbar wird diese implizite Norm in ihrer Ausprägung als ›prototypical whiteness‹ (Browne 2015) beispielsweise bei Gesichtserkennungssoftware. Gesichter dunkler Hautfarbe haben es schwerer, als Gesicht erkannt zu werden als weisse – so schwer, dass Google-Fotos dunkelhäutige Menschen mit Gorillas verwechselt (Barr 2015). Das liegt unter anderem daran, dass Machine-Learning-Trainingsdatensätze Diversität unzureichend abbilden, und veranschaulicht nochmals, dass Daten keineswegs neutral, sondern von Menschenhand kreiert sind. Abhilfe können etwa bessere Trainingsdatensätze schaffen, die menschliche Vielfalt umfassen, da sie von Teams erstellt werden, die dieselbe Vielfalt repräsentieren (Buolamwini 2016).

Neben der Diskriminierung im Tech-Sektor sei hier auch die Daten-Klassengesellschaft erwähnt, in der zwar (fast) alle zur datenproduzierenden Schicht gehören, aber nur wenige die Mittel haben, Daten zu sammeln, und eine noch kleinere Elite fähig ist, diese auch auszuwerten und zu verwenden (Manovich 2011). Ausserdem tragen fehlende Daten bzw. die Untervertretung in den Daten zur algorithmischen Diskriminierung bei, ebenso wie strukturelle Ungleichheiten, die sich in Daten nicht einfach in Luft auflösen. Solche rassifizierte, sexualisierte und gegenderte Ergebnisse von Datenpraktiken sind Bestandteil einer Stratifizierung, die Lyon (2003) treffend als ›social sorting‹ beschreibt. Wenn Algorithmen dann Menschen Wert oder Risiko zuschreiben, entstehen Diskriminierungen, die sich direkt auf die (Über)Lebenschancen auswirken können. Überwachung ist nicht nur in Sachen Privatsphäre ein Thema, sondern auch in Bezug auf soziale Gerechtigkeit.

Nichts zu verbergen?

Wer nichts zu verbergen hat, hat auch nichts zu befürchten – so wird die Massenüberwachung oft gerechtfertigt. Snowden kontert, nach diesem Muster könne man ebenso argumentieren, die freie Meinungsäusserung sei nicht so wichtig, weil man nichts zu sagen habe. Nichts zu verbergen zu haben, ist aber auch ein Privileg: Wer wie viel preisgeben kann, ohne dabei die eigene Sicherheit aufs Spiel zu setzen, entscheiden oft heteronormative Institutionen innerhalb militarisierter Grenzen, die ihren eigenen rassifizierten und sexualisierten Logiken folgen.

Für Transgender-Menschen zum Beispiel werden Fragen der (Un)Sichtbarkeit auf verschiedenen Ebenen problematisch. Das Bedürfnis nach Unsichtbarkeit trifft einerseits auf Gerichts- und Krankenakten, deren Vertraulichkeit stets in Frage steht. Andererseits muss sich auch die gefügige Sichtbarkeit der Kritik der Teilhabe (complicity) an hegemonialen Diskursen der nationalen Sicherheit stellen (Beauchamp 2009). ›Passing‹ bezieht sich hier neben dem Geschlecht auf weitere binär geprägte Grenzen. Wer sich als weisse/r, abschliessend gegenderte/r, sichere/r (zumindest aber sicher nicht als muslimische/r) Reisende/r ausweisen kann, passiert. Wem dies aber schwer fällt, der unterliegt erhöhtem Verdacht und verstärkter Überwachung. Die Schuld für die systemische Diskriminierung wird dabei auf ihre Opfer überwälzt: An allfälligen Negativfolgen sind sie selbst schuld, schliesslich hatten sie etwas zu verbergen (Andrejevic 2015).

Der Schutz der Privatsphäre ist nicht der einzige Zugang zum Thema Überwachung. Schliesslich sind weder die öffentliche Teilhabe noch die Privatsphäre, die als schützenswert gilt, gleich verteilt. Geflüchtete Men-

schen, sexuelle Minderheiten, Empfänger von Sozialleistungen, Menschen mit Behinderung oder Inhaftierte erfahren dies regelmässig am eigenen Leib (Dubrofsky/Magnet 2015). Es erscheint dabei aufschlussreich, dass das erhöhte öffentliche Interesse an Überwachungsthemen mit Enthüllungen zum Umfang der Massenüberwachung *aller* einhergeht, während die langjährige sexuelle, gegenderte und rassifizierte Überwachung marginalisierter Gruppen kaum Aufsehen erregte.

Intersektionelle Datenpraxis

Erprobte Kritik an Ungleichheiten und Machtbeziehungen, situiertes Wissen (Haraway 1988), starke Objektivität (Harding 1991), Intersektionalität und ein kritisches Verhältnis zur Privatsphäre sind bloss ein kleiner Auszug aus dem interdisziplinären feministischen Instrumentarium gegen ungerechte Auswirkungen der Datenpraxis und Überwachung. Die folgenden Vorschläge zur intersektionellen Datenpraxis bilden keine abschliessende Liste, sondern zeigen vielmehr mögliche Ausgangspunkte auf.

Die feministische Datenpraxis stützt sich auf die Handlungsfähigkeit und den Konsens derer, die zu Datenpunkten werden. Sie stellt sich damit gegen jede nicht einvernehmliche Datenerhebung und -verwendung, fördert Datenprojekte, die Minderheiten ermächtigen, legt Wert auf den Schutz von Daten, Privatsphäre und der Anonymität aller AkteurInnen und wirkt algorithmischen Diskriminierungen entgegen. Sie betrachtet Datenstrukturen als Machtstrukturen, hinterfragt die Annahmen, die Kategorien und Klassifikationen zugrunde liegen, und setzt sich auch mit Ausreissern und fehlenden Daten auseinander. Denn was im Grossen als unerhebliche Abweichung gehandhabt wird, kann im Kleinen Diskriminierung und Exklusion bedeuten.

Wissen – auch Daten sind Wissen – ist situiert und kontextabhängig. Die Überwachung intersektionell zu denken, ist ein Lernprozess, bei dem es unter anderem darum geht, die jeweilige Datenpolitik und die oft impliziten Machtverhältnisse kritisch zu hinterfragen: Wer ist in der Position, Daten zu sammeln und auszuwerten? Wessen Daten werden zu welchem Zweck gesammelt? Ermächtigen die Daten marginalisierte Menschen zu mehr Selbstbestimmung, zur informierten Ausübung ihrer Rechte? Oder festigen sie bestehende Machtstrukturen und grenzen andere weiter aus? Wie wird Konsens gehandhabt? Wer kann zustimmen, wer sich ausnehmen, wer wird von vornherein mehr als Datenpunkt denn als Mensch betrachtet? Aber auch: Wer fehlt in den Daten und wer wird dadurch einmal mehr zur impliziten Norm?

Überwachung wird meist gross gedacht: Massenüberwachung von

Kommunikationsdaten, Social Media, Überwachungsdrohnen oder Videoüberwachung. Intersektionelle Ansätze weisen dabei auf algorithmische Diskriminierung hin, stellen Zusammenhänge zwischen alten und neuen Formen der Datensammlung und Überwachung (wieder) her und heben hervor, dass Massenüberwachung zwar alle betrifft, sich aber nicht auf alle gleichermassen auswirkt. Nicht jede/r verfügt über das technologische Kapital, sich vor Dataveillance zu schützen. Auch hier wird, wer bereits an den Schnittstellen von Gender, ›Rasse‹ oder sozialer Schicht benachteiligt ist, zusätzlich ausgeschlossen, weil Bildung und Wissen zur digitalen Sicherheit auch ungleich verteilt sind.

Eine intersektionelle Datenpraxis denkt Überwachung aber auch mal klein und berücksichtigt Formen der Überwachung, die im öffentlichen Diskurs kaum Beachtung finden. Die Essays im Sammelband *Feminist Surveillance Studies* beschäftigen sich neben allgemeineren Interventionen in die Überwachungsforschung zum Beispiel auch mit Geburtsurkunden von Trans-Personen, transnationaler Leihmutterschaft, Reproduktionstechnologien oder der Überwachung von Kunden der Sexarbeit (Dubrofsky/Magnet 2015). Symptomatisch: während die NSA-Leaks und deren Folgen – letztens z.B. die WannaCry(pt) Ransomware – internationale Schlagzeilen machen, erscheint die schleichende Ausbreitung sogenannter ›Stalkerware‹ – oft Wegbereiter häuslicher Gewalt – kaum der Rede wert.[5]

Und letztlich: Wo Macht ist, ist auch Widerstand (Foucault 1978). Feministische Überwachungskritik kann durchaus auch bedeuten, sich der Überwachung kreativ zu widersetzen, zum Beispiel mit Unterwachung (Mann 2004), Experimentieren mit Kleidung gegen Überwachungsdrohnen und Make-up gegen Gesichtserkennung[6] oder mit feministischer Datensicherheit zum Selbermachen.[7]

Anmerkungen

1 Siehe Vortrag https://youtu.be/v1d0Xa2njVg.
2 N.P. v. Standard Innovation (US) Corp. d/b/a We-Vibe, Case No. 1:16-cv-08655.
3 Weder Gender noch Sexualität passieren in Isolation. Eine intersektionelle Perspektive auf Überwachung berücksichtigt daher auch andere Differenzierungen, so z.B. ›Rasse‹, Religion oder soziale Schicht.
4 Siehe z.B. https://youtu.be/d16LNHIEJzs
5 Siehe hierzu die Motherboard Serie *When Spies Come Home*, https://motherboard.vice.com/en_us/topic/when-spies-come-home
6 Siehe u.a. Projekte von Adam Harvey auf https://ahprojects.com/projects/
7 Siehe https://hackblossom.org/cybersecurity/

Literatur

Alexander, L. (2016): Do Google's ›unprofessional hair‹ results show it is racist? The Guardian.

Andrejevic, M. (2015): Foreword. In: R. E. Dubrofsky; S. A. Magnet (eds.): Feminist Surveil-

lance Studies. Andrejevic, M. (2005): The work of watching one another: Lateral surveillance, risk, and governance. Surveillance & Society, 2(4), pp. 479–497.
Barr, A. (2015): Google mistakenly tags black people as ›gorillas‹, showing limits of algorithms. Wall Street Journal.
Beauchamp, T. (2009): Artful Concealment and Strategic Visibility: Transgender Bodies and U. S. State Surveillance After 9/11. Surveillance & Society, 6(4), pp.356–366.
Browne, S. (2015): Dark Matters: On the Surveillance of Blackness. Durham: Duke University Press.
Buolamwini, J. (2016): How I'm fighting bias in algorithms. TED talk.
Caliskan, A.; Bryson, J.J.; Narayanan, A.; (2017: Semantics derived automatically from language corpora necessarily contain human biases. Science, 183–186(April), pp.183–186.
Conrad, K. (2009): Surveillance, Gender and the Virtual Body in the Information Age. Surveillance & Society, 6(4), pp.380–387.
de Freytas-Tamuramarch, K. (2017): Maker of ›Smart‹ Vibrators Settles Data Collection Lawsuit for $3.75 Million. The New York Times.
Dubrofsky, R.E.; Magnet, S.A. (eds.) (2015): Feminist surveillance studies. Durham: Duke University Press.
Foucault, M. (1978): The History of Sexuality: An Introduction. New York: Pantheon.
Gitelman, L. (ed.) (2013). ›Raw Data‹ is an Oxymoron. Cambridge, MA: MIT Press.
Haraway, D.J. (1988): Situated Knowledges: The Science Question in Feminism and the Privilege of Partial Perspective. Feminist Studies, 14(3), pp.575–599.
Harding, S. (1991): Whose Science? Whose Knowledge? Thinking from Women's lives. Ithaca: Cornell University Press.
Horton, H. (2016): Microsoft deletes ›teen girl‹ AI after it became a Hitler-loving sex robot within 24 hours. The Telegraph.
Kitchin, R. (2014): Big Data, new epistemologies and paradigm shifts. Big Data & Society, 1(1), pp.1–12.
Lyon, D. (2003): Surveillance as social sorting: computer codes and mobile bodies. In D. Lyon (ed.): Surveillance as Social Sorting: Privacy, risk, and digital discrimination. London: Routledge, pp. 13–30.
Magnet, S. (2011): When Biometrics Fail: Gender, Race, and the Technology of Identity. Durham: Duke University Press.
Magnet, S.; Rodgers, T. (2012): Stripping for the State: Whole body imaging technologies and the surveillance of othered bodies. Feminist Media Studies, 12(1), pp.101–118.
Mann, S. (2004): ›Sousveillance‹, Inverse Surveillance in Multimedia Imaging. In: Proceedings of the 12th annual ACM international conference on Multimedia, pp. 6(20–627.
Manovich, L. (2011): Trending: The Promises and the Challenges of Big Social Data. In: M. K. Gold (ed.): Debates in the Digital Humanities. Minneapolis: University of Minnesota Press, pp. 1–17.
McClintock, A. (1995): Imperial Leather: Race, Gender and Sexuality in the Colonial Contest. New York: Routledge.
Monahan, T. (2009): Dreams of Control at a Distance: Gender, Surveillance, and Social Control. Cultural Studies <-> Critical Methodologies, 9(2), pp.286–305.
Raley, R. (2013): Dataveillance and Countervailance. In: L. Gitelman (ed.): ›Raw Data‹ is an Oxymoron.
Rizk, V.; Othman, D. (2016: Quantifying Fertility and Reproduction through Mobile Apps: A Critical Overview. Arrow for Change, 22(1).
Smith, A. (2015): Not-Seeing: State Surveillance, Settler Colonialism and Gender Violence. In: R. E. Dubrofsky; S. A. Magnet (eds.): Feminist Surveillance Studies, pp. 21–38.
Stoler, L. (2010): Carnal Knowledge and Imperial Power: Race and the Intimate in Colonial Rule. Berkeley: University of California Press.
UN OHCHR (2014): The Right to Privacy in the Digital Age. undocs.org/A/HRC/27/37.
van der Ploeg, I. (2012): The body as data in the age of information. In: K. Ball; K. D. Haggerty; D. Lyon (eds.): Routledge Handbook of Surveillance Studies. Oxon: Routledge, pp. 176–183.
van der Ploeg, I. (2003): Biometrics and the body as information. In: D. Lyon (ed.): Surveillance as social sorting: computer codes and mobile bodies.