Zeitschrift für Medienwissenschaft, Jg. 18, Heft 34 (1/2026), https://doi.org/10.14361/zfmw-2026-180107. Published by transcript Verlag.

TATJANA SEITZ

BEQUEMLICHKEITSARCHITEKTUREN

Eine API-Kritik am Beispiel der Facebook-Login-Experience

Anwendungsprogrammierschnittstellen (*application programming interfaces*, APIs) sind zu zentralen Elementen geworden, die Plattformökonomien und den digitalen Alltag organisieren. Eng verflochten mit dem Aufstieg der Plattform als dominierendem technologischen und ökonomischen Modell des datafizierten Webs[1] stehen APIs heute nahezu synonym für den Austausch von Daten und Diensten zwischen Unternehmen, Datenservern und Software/Apps. Plattformen ermöglichen über APIs programmierbaren Zugriff auf Unternehmensressourcen, sodass Drittparteien diese nutzen können, um auf der digitalen Infrastruktur der Plattform aufzubauen. Gleichzeitig fungieren APIs – über die Kontrolle der Bedingungen für Innovation – als Mittel zur Steuerung von Drittanwender*innen-Apps. APIs dominanter Plattformanbieter*innen wie Facebooks Graph API sind jedoch keine stabilen digitalen Objekte. Sie modulieren fortlaufend die Bedingungen, unter denen Software-Entwicklung möglich ist, sowie die Modi infrastruktureller Kontrolle.[2] Anhand von APIs lässt sich daher nachvollziehen, wie Plattformen Macht durch eine Logik gleichzeitiger Ermöglichung und Begrenzung ausüben: Zum einen schaffen sie neue Möglichkeiten der Software-Entwicklung und ökonomischen Partizipation, zum anderen üben sie Kontrolle aus, indem sie Datenflüsse formen und gesellschaftliche Konzepte – wie etwa Datenschutz – hervorbringen.

Eine zentrale Komponente der heutigen Web- und App-Architektur ist die Identifizierung von Personen über Social-Media-Nutzer*innenprofile und die Autorisierung des API-Zugriffs über von digitalen Plattformen bereitgestellte Social Logins. Die Login-Funktion von Facebook ist sowohl bei Nutzer*innen als auch bei App-Entwickler*innen beliebt. Facebook stellt Entwickler*innen eine vorgefertigte Login-Funktion zur Verfügung, die entweder als Code oder als SDK (Software Development Kit) in externen Apps und Webseiten implementiert werden kann. Nutzer*innen können sich mit ihr bei Apps und Diensten anmelden, ohne jeweils ein neues Profil erstellen zu müssen. App-Entwickler*innen hingegen erhalten über

1 Vgl. Anne Helmond: The Platformization of the Web. Making Web Data Platform Ready, in: *Social Media + Society*, Bd. 1, Nr. 2, 2015, 1–11, doi.org/10.1177/2056305115603080.

2 Vgl. Ganaele Langlois u. a.: Networked Publics. The Double Articulation of Code and Politics on Facebook, in: *Canadian Journal of Communication*, Bd. 34, Nr. 3, 2009, 415–434, doi.org/10.22230/cjc.2009v34n3a2114; Carolin Gerlitz, Anne Helmond: The Like Economy. Social Buttons and the Data-Intensive Web, in: *New Media & Society*, Bd. 15, Nr. 8, 2013, 1348–1365, doi.org/10.1177/1461444812472322.

3 Vgl. dazu die fortlaufende Dokumentation des Verfahrens FTC vs. Facebook, Inc. auf der Website FTC.gov (ftc.gov/legal-library/browse/cases-proceedings/092-3184-182-3109-c-4365-facebook-inc-matter), hier insb. das Dokument Exhibit A–Exhibit S [Beweisstücke für Facebooks irreführende Datenschutzversprechen], 27.7.2011, ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookexha-s.pdf (3.12.2025).

den Login die Möglichkeit, über die Graph API programmierbaren Zugriff auf Nutzer*innendaten anzufordern. Als wesentliches Element von Facebooks digitaler Datenschutzinfrastruktur war die Login-Funktion zudem ein zentraler Gegenstand von langjährigen Untersuchungen zu Verstößen gegen den Datenschutz durch Facebook (2011–2019).[3]

In starkem Kontrast dazu steht die 2014 erfolgte Wiedereinführung eines bedienfreundlichen Datenschutzmodells durch Facebook als eine «login experience», die auf dem Entwickler*innen-Blog des Unternehmens als «fast and convenient» beworben wurde.[4] Lässt sich die hier wirkende Bequemlichkeitslogik, also die Überführung der Datenschutzanforderungen in eine Logik der bedienfreundlichen Komfortorientierung, tatsächlich so spannungsfrei realisieren, wie es Facebook nahelegt? Gerade die Entwicklungen des Plattform-Kapitalismus, in dem – wie unter anderem der Ökonom Nick Srnicek betont hat – die Ausweitung der Kapazitäten zur Datenerfassung als «competitive imperative for these companies» verstanden werden kann,[5] erfordern eine kritische Betrachtung der Bequemlichkeitslogik in datenintensiven Plattformökonomien. Eine genauere Betrachtung zeigt, dass der Übergang vom Facebook-«Login» zur «Login-Experience» Teil eines systematischen *experience shift* ist, die darauf abzielt, die Graph API sowie andere Services und Werkzeuge für Entwickler*innen sukzessive nach den Prinzipien des User Experience Designs neu zu gestalten. Meine eigene Auswertung von Mark Zuckerbergs Keynotes auf der Entwicklerkonferenz *F8* (2008–2021) zeigt beispielsweise, dass bei der Vorstellung der Graph API und Services und Werkzeuge für Entwickler*innen der Begriff «experience» zu einem der am häufigsten verwendeten Begriffen zählt – direkt nach «platform».[6] Vor diesem Hintergrund scheint es naheliegend, die Übersetzung der Datenschutzarchitektur in eine Bequemlichkeitslogik als Beispiel für eine umfassende Transformation der Plattforminfrastruktur durch User Experience Design zu betrachten. Doch was bedeutet es, Programmierschnittstellen und andere Werkzeuge für Entwickler*innen wie den Login bedienfreundlicher zu gestalten? Diesem Phänomen – der Umgestaltung der Graph API nach den Prinzipien und Techniken des User Experience Designs – nähert sich dieser Beitrag durch die Analyse der Login-Experience.

Am Beispiel des Übergangs vom «Login» zur «Login-Experience» bei Facebook werden die spezifischen Bedingungen, unter denen der Datenschutz zur Frage der Bequemlichkeit wird, beleuchtet. Dabei verfolgt der Beitrag einen *designerly*-Ansatz, der das im User Experience Design verankerte Wissen sowie die spezifischen Techniken aus Theorie und Praxis der Human Computer Interaction (HCI) in eine kritische Analyse einbezieht.[7] Um den Login-Prozess im praktischen Vollzug zu realisieren, müssen Interfaces, Datenbanken, Datenströme, gesetzliche Vorschriften, ökonomische Interessen, Berechtigungen und Klicks in einer konkreten Abfolge zusammengeführt werden – so wird der ‹Benutzer*innenfluss› für den Anmeldevorgang bzw. der Login-User-Flow erzeugt. Konkret schlägt dieser Beitrag daher einen kritischen Zugang mittels

4 Jeffrey Spehar: The New Facebook Login and Graph API 2.0 [Beitrag auf Unternehmensblog], *Facebook Developers Blog*, 30.4.2014, *developers.facebook.com/blog/post/2014/04/30/the-new-facebook-login* (3.12.2025).

5 Nick Srnicek: *Platform Capitalism*, Cambridge (UK) 2016, 102.

6 Für diese Analyse wurden automatisierte Transkripte von F8-Videos aus den Jahren 2008–2021 erstellt (insgesamt neun Konferenzen), die auf YouTube gefunden wurden (eine Aufzeichnung der ersten F8-Konferenz aus dem Jahr 2007 wurde nicht gefunden; in den Jahren 2009, 2012 und 2013 fand die Konferenz nicht statt. Seit 2014 wird die F8 jährlich im Frühjahr abgehalten. Die Transkripte der Jahre 2008 und 2010 sind nicht vollständig, enthalten jedoch den Großteil der Keynotes von Mark Zuckerberg. Für die Jahre 2011 bis 2021 – mit Ausnahme von 2012 und 2013 – liegen vollständige Transkripte der Keynotes sowie Beiträge weiterer Unternehmensvertreter*innen vor). Die Videos wurden mithilfe des Browser-Tools *youtubetranscript.com* transkribiert. Die Transkripte wurden nicht manuell editiert, da das primäre Ziel darin bestand, Trends, Muster, Anomalien und Häufigkeiten in einem umfangreichen textbasierten Datensatz sichtbar zu machen. Manuell bereinigt wurden lediglich sehr häufig vorkommende, umgangssprachliche und formatspezifische Wörter wie «more», «go», «now», «want», «new», «really», «one», «make», «thing», «way», «year», «today» und «see». Zudem habe ich «experience» im Singular und «experiences» im Plural zusammengeführt.

7 Vgl. Michael Dieter, Nathaniel Tkacz: The Patterning of Finance/Security. A Designerly Walkthrough of Challenger Banking Apps, in: *Computational Culture*, Nr. 7, Jan. 2020, *computationalculture.net/the-patterning-of-finance-security* (14.12.2025).

designerly-User-Flows vor, um mithilfe der User-Experience-Design-Technik den User Flow zu untersuchen, insbesondere daraufhin, wie Datenschutz bei Facebook als eine *experience* im Sinne einer bestimmten Bequemlichkeitslogik gedacht und umgesetzt wird. Durch «multi-situated» User Flows wird das Facebook-Modell eines bedienfreundlichen Datenschutzes methodisch untersucht.[8] Die Analyse zeichnet nach, wie Datenschutz so umgestaltet wird, dass er sich mühelos in die Gewohnheiten des digitalen Alltags einfügt, zugleich jedoch die wirksame Regulierung der Produktion, Analyse oder Zirkulation von Datenströmen praktisch aushebelt.

Dieser Beitrag gliedert sich in drei Abschnitte: Der erste setzt sich kritisch mit der Bequemlichkeitslogik aus der Perspektive des User Experience Designs auseinander und führt die Methode des *designerly*-User-Flows ein. Der zweite Abschnitt analysiert Facebooks Übergang zur Login-Experience, indem er das infrastrukturelle Setting durch *designerly*-User-Flows wiederholt (neu-)verortet, um die stabilisierenden Bedingungen der Bequemlichkeitslogik freizulegen. Abschließend behandelt der dritte Abschnitt kurz die permanente Modulation als Wirkungsweise bedienfreundlicher Formen der Governance innerhalb datenintensiver digitaler Infrastrukturen.

Gegen die Bequemlichkeit: «designerly»-User-Flows als API-Kritik

Dass sämtliche Bereiche des digitalen Lebens von einer Rhetorik der *experience* durchdrungen werden, ist Michael Dieter und Nathaniel Tkacz zufolge kein Zufall, sondern «a deliberate strategy of app design».[9] Unterschiedliche Aktivitäten, Praktiken, soziale Regeln und regulatorische Rahmenbedingungen werden, so die beiden Medienwissenschaftler, «reworked», indem sie durch den «experience layer» neu konfiguriert werden.[10] An diesem Prozess der Neukonfiguration, so argumentiert Dieter an anderer Stelle weiter, ist User Experience Design beteiligt, indem es Potenziale in etwas Wahrnehmbares, Programmierbares oder Handhabbares überführt.[11] Die analytische Figur des *experience layer* rekurriert dabei auf ein spezifisches Verständnis des Interface als einer fluiden Form von Governance.[12] Vor diesem Hintergrund wird die Transformation des «interface into a surface» durch Techniken und Kenntnisse des User Experience Designs als «indirect mode of control externally imposed by design» konzeptualisiert.[13] Die Prominenz des Begriffs *experience* und mit ihm assoziierter Schlüsselbegriffe wie *seamlessness*, *convenience* und *personalisation* wirft daher die Frage auf, weshalb *experience* im Kontext von APIs eine besondere Rolle spielt – und welche Formen von Handlungsmacht Plattformbetreiber*innen dadurch erlangen, die nicht bereits im technologischen und ökonomischen Modell der ‹Plattform› angelegt sind.[14] Folglich wird API-Design hier als eine Zone der Governance und des Aushandelns verstanden, deren kritische Untersuchung Einblicke in Designtechniken und das ihnen zugrunde liegende Wissen erfordert.

8 Vgl. Michael Dieter u. a.: Multi-Situated App Studies. Methods and Propositions, in: *Social Media + Society*, Bd. 5, Nr. 2, 2019, 1–15, doi.org/10.1177/2056305119846486.

9 Dieter, Tkacz: The Patterning of Finance/Security.

10 Ebd.

11 Vgl. Michael Dieter: Interface Critique at Large, in: *Convergence*, Bd. 30, Nr. 1, 2022, 49–65, doi.org/10.1177/13548565221135833.

12 Vgl. Branden Hookway: *Interface*, Cambridge (MA) 2014.

13 Dieter: Interface Critique at Large, 55.

14 Vgl. Jean-Charles Rochet, Jean Tirole: Platform Competition in Two-Sided Markets, in: *Journal of the European Economic Association*, Bd. 1, Nr. 4, 2003, 990–1029, doi.org/10.1162/154247603322493212; Tarleton Gillespie: The Politics of «Platforms», in: *New Media & Society*, Bd. 12, Nr. 3, 2010, 347–364, doi.org/10.1177/1461444809342738; Helmond: The Platformization of the Web; Rory Van Loo: The New Gatekeepers: Private Firms as Public Enforcers, in: *Virginia Law Review*, Bd. 106, Nr. 2, 2020, virginialawreview.org/articles/new-gatekeepers-private-firms-public-enforcers/ (14.12.2025).

Die Einführung der Login-Experience durch Facebook als «schneller und bequemer Weg» der Anmeldung bei Apps erfolgte alles andere als zufällig.[15] Vielmehr ist sie als Form der ‹Präfiguration› zu verstehen, die Bequemlichkeit dadurch erzeugen soll, dass Datenschutz antizipativ durch routinierte Praktiken des Klickens und Fließens hergestellt wird.[16] Im User Experience Design verweist die Komfortorientierung (*convenience*) auf einen systematischen Ansatz, der darauf abzielt, den Handlungsraum dergestalt zu strukturieren, dass Mensch-Computer-Interaktionen als intuitiv und mühelos wahrgenommen werden. Die Bequemlichkeitslogik erfasst, wie Werte in diesen Interaktionen bestimmt und durch spezifische Techniken umgesetzt werden; sie schafft handlungsleitende Kategorien und formt das Beziehungsgefüge. Beispielsweise gelten Interaktionen als vorteilhaft, die eine Zielvorgabe schnell, mühelos und intuitiv erfüllen. Prozesse, die bewusste Aufmerksamkeit, Erkundung oder kontemplative Reflexion erfordern, werden hingegen als frustrierend, verwirrend, inkonsistent und letztlich unerwünscht angesehen.

Obwohl Facebooks Login-Experience Nutzer*innen ein schnelleres Anmelden bei Apps und Entwickler*innen den Zugriff auf die Graph API in nur wenigen Schritten ermöglicht, schränkt die komfortorientierte Gestaltung von Nutzungspraktiken laut der Netzkünstlerin und Designkritikerin Olia Lialina zugleich die Handlungsfähigkeit, Wissensaneignung und den affektiven Erfahrungsraum der Nutzer*innen ein.[17] Für Lialina liegt der Wert offener Systeme gerade darin, Nutzer*innen die Möglichkeit zu geben, Elemente zu manipulieren, Wissen zu erwerben, sich beteiligt zu fühlen oder auch überwältigt zu werden. Heute wird ein solch exploratives oder ungerichtetes Verhalten jedoch zunehmend als irrational, inkonsistent und unvorhersehbar und damit als unerwünscht umgedeutet, da es sich der ökonomischen Verdatungslogik entzieht.[18] Unter dem Einfluss der Verhaltensökonomie und der kognitiven Psychologie unterstützt dieser Wandel im Forschungsgebiet der Mensch-Computer-Interaktion den im User Experience Design vorherrschenden Ansatz, nach dem Nutzer*innen kontinuierlich in ihrem Handeln angeleitet werden müssen. Infolgedessen bieten optimierte Websites und Apps oft nur den einen ‹richtigen› Weg, um fortzufahren, und legen im Voraus fest, welche handlungsbezogenen, verhaltensbezogenen und affektiven Potenziale realisiert werden können.

User Flows sind eine Methode des User Experience Designs und Interaktionsdesigns, die verwendet wird, um aufgabenorientierte Abläufe vorab so zu konfigurieren, dass Nutzer*innen sich mühelos in digitalen Systeme bewegen können. Sie sind darauf ausgerichtet, Bedienfreundlichkeit herzustellen, indem sie die Nutzung eines User Interface so einfach wie möglich gestalten.[19] In diesem Sinne machen User Flows Aktionen nachvollziehbar, programmierbar und umsetzbar, sodass sie in der Praxis durch Klicken und Wischen in einem nahtlosen Interaktionsablauf (*flow*) ausgeführt werden können. Die Nielsen Norman Group, eine der führenden Institutionen in Forschung und Ausbildung im Bereich User Experience Design, definiert User Flow wie folgt:

15 Vgl. Spehar: The New Facebook Login and Graph API 2.0.

16 Vgl. Dieter: Interface Critique at Large.

17 Vgl. Olia Lialina: Turing Complete User, in: *Contemporary Home Computing*, Oktober 2012, contemporary-home-computing.org/turing-complete-user (3.12.2025).

18 Vgl. B. J. Fogg: Persuasive Technologies, in: *Communications of the ACM*, Bd. 42, Nr. 5, Mai 1999, 26–29, doi.org/10.1145/301353.301396; Richard H. Thaler, Cass R. Sunstein: *Nudge. Improving Decisions about Health, Wealth, and Happiness*, New Haven 2008; Nir Eyal: *Hooked. How to Build Habit-Forming Products*, New York 2014; Steve Krug: *Don't Make Me Think, Revisited. A Common Sense Approach to Web Usability*, 3. Aufl., Berkeley 2014; Cliff Kuang, Robert Fabricant: *User Friendly. How the Hidden Rules of Design Are Changing the Way We Live, Work, and Play*, New York 2019.

19 Ergonomics of human-system interaction – Part 210: Human-centred design for interactive systems (ISO 9241-210:2010(en)), *International Organization for Standardization*, 2010, iso.org/obp/ui/#iso:std:iso:9241:-210:ed-1:v1:en (3.12.2025).

«A *user flow* is a set of interactions that describe the typical or ideal set of steps needed to accomplish a common task performed with a product.»[20] Zu diesem Zweck stützen sich User Flows auf Erkenntnisse aus der Positiven Psychologie, der Kognitiven Psychologie und des Cognitive Engineering und modellieren sie anhand von Designmethoden und Datenerhebungsverfahren aus der HCI.[21] Leicht bedienbar gestaltete User Flows lassen sich mit dem Begriff des psychologischen *flows* von Mihály Csíkszentmihályi fassen, der sich seit den 1970er Jahren mit dem Phänomen beschäftigt hat.[22] Nach Csíkszentmihályi bezeichnet *flow* einen Geisteszustand, in dem eine Person so vollständig in eine angenehme oder freudige Tätigkeit eintaucht, dass sich ihr Zeitgefühl und ihr bewusstes Handeln verändern.[23] Gestützt auf Csíkszentmihályis Arbeit entwirft der Design- und Medienwissenschaftler Braxton Soderman in *Against Flow* eine kritische Theorie des kognitiven Flows als einer zentralen *mastery* in modernen kapitalistischen Gesellschaften, die «flowing subjects» als produktiver ansehen.[24] In neoliberalen Gesellschaften, in denen Produktivität gefragt ist und die statt kollektiver Solidarität die individuelle Verantwortung fördern, so Soderman, erleichtert die Überwindung von ‹Störungen› wie «disorder and blockage» eine «more continuous and unified experience», mit dem Potenzial, unproduktive Aktivitäten wie das Spielen in Selbstoptimierungstechniken zu verwandeln.[25] Mithilfe der Flow-Theorie werden User Flows optimiert, um Nutzer*innen reibungslos durch digitale Infrastrukturen zu führen und die Integration gesetzlicher Rahmenbedingungen und die Produktion von Ergebnissen zugleich praktisch zu gestalten. Doch wie kann eine kritische Auseinandersetzung mit User Flows aussehen?

Plattformen und ihre APIs bieten spezifische Forschungsaffordanzen, die es erlauben, die Bequemlichkeitslogik kritisch zu untersuchen. Die hier dargelegte API-Kritik folgt einem Ansatz der «inventive methods»,[26] bei dem Elemente der Bequemlichkeitslogik methodisch eingesetzt werden, um die Login-Experience als einen Ort der kritischen Untersuchung herzustellen.[27] Walkthroughs sind eine weitere Methode des User Experience Designs, die in der Medienwissenschaft zunehmend als methodischer Zugriff eingesetzt wird.[28] Bei Walkthroughs handelt es sich nicht um eine Technik des Gestaltens von Interaktionen im engeren Sinne, sondern vielmehr um eine branchenweit etablierte Form der «sequential analysis of usability».[29] Sowohl Walkthroughs als auch User Flows sind Werkzeuge des User Experience Designs; sie unterscheiden sich jedoch in Zweck und Format und eröffnen unterschiedliche Möglichkeiten für kritische Forschung und Analyse. Walkthroughs eignen sich besonders gut, um die erstmalige Interaktion von Nutzer*innen mit einer App – etwa das Einrichten eines neuen Benutzer*innenkontos (*onboarding*) – in einen Forschungsrahmen zu überführen.[30] Wie jedoch die Analyse im nächsten Abschnitt zeigt, ist Datenschutz bei Facebook genau dann bequem, wenn er als Teil alltäglicher Aktivitäten verhandelt wird und nicht während eines zentralen Prozesses wie dem erstmaligen Einloggen in eine neue App. Deshalb konzentriert sich die

20 Kate Kaplan: User Journeys vs. User Flows [Beitrag auf Unternehmensblog], *Nielsen Norman Group*, 16.4.2025, nngroup.com/articles/user-journeys-vs-user-flows (3.12.2025).

21 Vgl. Braxton Soderman: *Against Flow. Video Games and the Flowing Subject*, Cambridge (MA) 2021; Karen Yeung: «Hypernudge». Big Data as a Mode of Regulation by Design, in: *Information, Communication & Society*, Bd. 20, Nr. 1, 2017, 118–136, doi.org/10.1080/1369118X.2016.1186713; Donald A. Norman: *The Design of Everyday Things*, New York 1988.

22 Vgl. Mihaly Csíkszentmihályi: *Flow: The Psychology of Optimal Experience*, New York 1991.

23 Vgl. Csíkszentmihályi: The Conditions of Flow, in: ders.: *Flow*, 71–93, hier 71.

24 «Flowing subjects», so Soderman, «are not simply game players experiencing the psychological state of flow; they are being positioned as media consumers in a way that promotes flow's ideologies». Soderman: *Against Flow*, 6.

25 Ebd., 42.

26 Celia Lury, Nina Wakeford (Hg.): *Inventive Methods. The Happening of the Social*, New York 2012.

27 Vgl. Noortje Marres: The Redistribution of Methods: On Intervention in Digital Social Research, Broadly Conceived, in: *The Sociological Review*, Bd. 60, Nr. 1 (Supplement), 2012, 139–165, doi.org/10.1111/j.1467-954X.2012.02121.x; dies., Carolin Gerlitz: Interface Methods. Renegotiating Relations between Digital Social Research, STS and Sociology, in: *The Sociological Review*, Bd. 64, Nr. 1, 2016, 21–46. doi.org/10.1111/1467-954X.12314; Dieter u. a.: Multi-Situated App Studies.

28 Vgl. Ben Light, Jean Burgess, Stefanie Duguay: The Walkthrough Method. An Approach to the Study of Apps, in: *New Media & Society*, Bd. 20, Nr. 3, 2018, 881–900, journals.sagepub.com/doi/10.1177/1461444816675438; Dieter, Tkacz: The Patterning of Finance/Security.

29 Dieter, Tkacz: The Patterning of Finance/Security.

30 Vgl. ebd.

Analyse in diesem Beitrag auf User Flows. Strategisch angewandt, kann ein *designerly*-User-Flow dazu dienen, dem «infrastrukturellen Setting» der Bequemlichkeitslogik als einem sinnvollen Datenschutzmodell entgegenzuwirken und es zugleich wirksam zu nutzen, um verschiedene Forschungsszenarien zu erzeugen.[31] *Designerly*-User-Flows fungieren dabei als historisch situierte, kontextuelle und relationale methodische ‹Interventionen›.[32] Sie zielen darauf ab, die Normalisierung der Komfortlogik als eine sinnvolle Form des Schutzes der digitalen Privatsphäre strategisch zu hinterfragen, zu untersuchen und sich gegebenenfalls einer solchen Normalisierung zu widersetzen.[33] Da User Flows jedoch auf einer bestimmten sequenziellen Anordnung von visuellen, haptischen, sensorischen und affektiven Affordanzen beruhen, die leichte Bedienbarkeit durch subtile *nudges* herstellen, benötigen sie selbst eine Mapping-Methode, um das soziotechnische Gefüge sichtbar zu machen. Für die Analyse werden daher Walkthroughs herangezogen, um User Flows nachzuzeichnen und so analysierbar zu machen.[34] Es folgt eine Analyse der Login-Experience bei Facebook, um schrittweise ein kritisches Verständnis davon zu entwickeln, was es bedeutet, Datenschutz in datenintensiven Plattformökonomien im Sinne der Bequemlichkeitslogik zu gestalten, und zu erörtern, welche Rückschlüsse sich daraus auf bedienfreundliche Formen der Macht und Kontrolle von Plattformen ziehen lassen.

Die Bequemlichkeitslogik der Login-Experience

Im Jahr 2008 führte Facebook die Social-Login-Funktion «Facebook Connect» ein.[35] Drei Jahre später ersetzte die Plattform die unternehmenseigene Funktion der Authentifizierung und Autorisierung über HTTP durch das offene Autorisierungsprotokoll OAuth 2.0.[36] Social-Media-Login-Funktionen verwenden in der Regel dieses Protokoll zur Definition von Datenschutzarchitekturen für das Identitätsmanagement. Das OAuth-2.0-Protokoll ist ein speziell für Web-APIs entwickelter Industriestandard für die Berechtigungsdelegierung, der regelt, wie Anwendungen von Drittanbieter*innen im Namen von Nutzer*innen auf Daten einer anderen Anwendung zugreifen können. Dieser offene Standard, ursprünglich von der Social-Media-Plattform Twitter für ihre API initiiert, wurde entwickelt, um Apps von Drittentwickler*innen (Clients) den Zugriff auf Ressourcen zu ermöglichen, die von einem anderen Unternehmen (Ressourcenserver) gehostet werden und die die Genehmigung der Endnutzer*innen (Ressourcenbesitzer*innen) des Unternehmens erfordern, das die Ressourcen hostet. Dadurch können Websites und Apps auf die Social-Media-Profile von Nutzer*innen zugreifen, um ihre Dienste anzubieten, ohne dass ein Profil innerhalb der App erstellt werden muss. Die angeforderten Daten werden über eine API weitergegeben.

Das OAuth-2.0-Protokoll enthält zwei wesentliche Mechanismen: Der API-Scope-Mechanismus definiert die Zugriffsrechte, die für bestimmte Ressourcen

31 Vgl. Dieter u. a.: Multi-Situated App Studies.

32 Vgl. Marres: The Redistribution of Methods.

33 Vgl. ebd.

34 Vgl. Dieter, Tkacz: The Patterning of Finance/Security.

35 Dave Morin: Announcing Facebook Connect [Beitrag auf Unternehmensblog], *Facebook Developers* Blog, 9.5.2008, *web.archive.org/web/20120910000405/https://developers.facebook.com/blog/post/2008/05/09/announcing-facebook-connect* (3.12.2025).

36 Naitik Shah: Developer Roadmap Update: Moving to OAuth 2.0 + HTTPS [Beitrag auf Unternehmensblog], *Facebook Developers* Blog, 10.5.2025, *web.archive.org/web/20110518220515/https://developers.facebook.com/blog/post/497* (3.13.2025).

gewährt werden können. Zugriffsrechte werden in den Entwickler*innendokumenten von Facebook in der Regel als ‹Berechtigungen› (*permissions*) aufgeführt. Solche Berechtigungen – die weder einen Vertrag noch einen Standard darstellen – sind zu zentralen Mechanismen der Plattform-Governance geworden. Jennifer Pybus und Mark Coté, die untersuchen, wie personenbezogene Daten ökonomisch verwertbar gemacht werden, definieren Berechtigungen als «the basic instructions of a complex system of automated data sharing».[37] Der Standard definiert außerdem einen zweiten Mechanismus, den Einwilligungsdialog (*consent screen*). In diesem Graphical User Interface (GUI) werden den Nutzer*innen diejenigen Berechtigungen zur Zustimmung angezeigt, die zuvor von Drittentwickler*innen in den ‹Scopes› angefordert werden. Die Ausgestaltung des Einwilligungsdialogs wird in der Regel von der Plattform bestimmt. Der vom OAuth-2.0-Protokoll definierte Anmeldeprozess wird in einer Drittanbieter*innen-App initiiert, die Nutzer*innen zum Zustimmungsbildschirm der jeweiligen Ressourceninhaber*innen weiterleitet. Der Klick auf die Schaltfläche ‹OK› auf dem Zustimmungsbildschirm wird als Zustimmung zur Erteilung der Berechtigung interpretiert, was zur Generierung eines Zugriffstokens für den anfragenden Drittanbieter*innen führt.

Im Jahr 2011 verklagte die Federal Trade Commission (FTC) Facebook wegen Verletzung der Datenschutzversprechen gegenüber Verbraucher*innen und nachfolgend wegen wiederholter Verwendung irreführender Auskünfte und Einstellungen.[38] Während einer fast zehnjährigen Untersuchung, die 2019 mit einer «historic penalty» in Höhe von 5 Milliarden US-Dollar endete, nahm die Ausgestaltung des Datenzugriffsmechanismus eine zentrale Rolle in der politischen Debatte ein.[39] Sowohl 2012 als auch 2019 heißt es in der Verfügung der FTC: «[I]t is further ordered that […] prior to any sharing of a user's nonpublic user information […] with any third party [Facebook needs to] obtain the user's affirmative express consent.»[40] In Übereinstimmung mit den Anforderungen der FTC sind Berechtigungen und der Zustimmungsbildschirm zu wesentlichen Bestandteilen und zur offiziellen digitalen Version eines «informed consent» der Nutzer*innen geworden. Bei der Durchführung der Walkthroughs verschiedener User Flows der Login-Experience ergab sich ein wesentlicher Unterschied zwischen den Merkmalen des Industriestandards, der den Datenschutz in API-Architekturen interpretiert und definiert, und den vom Plattformbetreiber implementierten bedienfreundlichen technologisch-materiellen Komponenten und Verfahren, die die bestehenden Datenschutzinfrastrukturen im praktischen Vollzug modulieren.

Was die hauseigene Funktion «Facebook Connect» (2008–2011) betrifft, umfasste diese weder die Anzeige von Berechtigungen im Zustimmungsdialog (Abb. 1), noch gab es ein systematisches Verfahren zur Anforderung, Genehmigung oder Verwaltung von Berechtigungen. Mit der Aktualisierung der Anmeldefunktion im Jahr 2011 wurde die Verwaltung von Zugriffsrechten über das OAuth-Protokoll eingeführt. Die Aktualisierung der Anmeldefunktion

37 Jennifer Pybus, Mark Coté: Did You Give Permission? Datafication in the Mobile Ecosystem, in: *Information, Communication & Society*, Bd. 25, Nr. 11, 2021, 1650–1668, zit. n. Online-Version 1–19, hier 6, doi.org/10.1080/1369118X.2021.1877771.

38 Vgl. FTC: Complaint [Klageschrift im Verfahren betreffend Facebooks irreführender Datenschutzversprechen], *Federal Trade Commission*, 27.7.2011, ftc.gov/sites/default/files/documents/cases/2011/11/111129facebookcmpt.pdf (3.12.2025); Lesley Fair: FTC's $5 Billion Facebook Settlement: Record-Breaking and History-Making [Pressemitteilung], *Federal Trade Commission*, 24.7.2019, ftc.gov/news-events/blogs/business-blog/2019/07/ftcs-5-billion-facebook-settlement-record-breaking-history (3.12.2025).

39 Fair: FTC's $5 Billion Facebook Settlement.

40 FTC: Decision and Order [rechtlich bindende Verfügung im Verfahren betreffend Facebooks irreführender Datenschutzversprechen], *Federal Trade Commission*, 27.7.2012, ftc.gov/sites/default/files/documents/cases/2012/08/120810facebookdo.pdf (3.12.2025); FTC: Order Modifying Prior Decision and Order [Erweiterungen des Beschlusses von 2012], *Federal Trade Commission*, 27.4.2020, ftc.gov/system/files/documents/cases/c4365facebookmodifyingorder.pdf (3.12.2025).

im Jahr 2014 versprach, «to give people more control over the information they share with apps».[41] Dieses Versprechen resultierte nicht in einer neuen Datenschutzarchitektur, sondern modifizierte vielmehr den programmierbaren Handlungsraum.

Abb. 1 **Beispiel für ein Facebook-Connect-Dialogfenster ohne Zustimmungsbildschirm aus dem Jahr 2009**

Diachrone User Flows. Ein diachroner Walkthrough von Facebooks Login-Funktion nach OAuth-Protokoll vor 2014 (im Vergleich zum Zugriffsmanagement nach der Einführung der Login-Experience) zeigt bemerkenswerte Unterschiede zwischen dem empfohlenen Standard und Facebooks Umsetzung auf.[42] Besonders auffällig war der Umfang der Elemente und Prozesse, die vom Protokoll nicht ausdrücklich gefordert wurden. Eine Besonderheit dieser Optimierung der Graph API nach den Prinzipien einer leichteren Bedienbarkeit ist die ‹GUI-fizierung von Code› – die Umwandlung offener Programmierpraktiken in das, was der Informatiker und Internetkritiker Philip E. Agre als «grammar of action» (Grammatik des Handelns) bezeichnet hat.[43] Die im Scope-Mechanismus durch Kommata getrennten, aufgelisteten Berechtigungen wurden in GUIs überführt. Sie erscheinen als Dropdown-Menüs zur Auswahl von Berechtigungen, Schaltflächen zum Anklicken sowie Dialogfenster zum Hochladen von Informationen über Drittanbieter*innen-Apps (Abb. 2). Neben den für die Funktion des OAuth-Protokolls erforderlichen Berechtigungen umfasst der Ablauf nach 2014 eine Vielzahl von heterogenen Elementen wie Listen, Best-Practice-Beispiele, Beschreibungsfelder, Upload-Dialogfelder, Dateiauswahlfelder und Dropdown-Menüs. Eine weitere Änderung betrifft die Anzahl der zur Erledigung der Aufgabe ‹Berechtigungsanfrage› erforderlichen Schritte. Tatsächlich gab es unter Facebook Connect (2007–2011) überhaupt keine Berechtigungsanfrage (Abb. 1). Alle über den öffentlichen Teil der Graph API verfügbaren Informationen wurden automatisch immer geteilt. Vor 2014 wurde die Berechtigungsanfrage der Anmeldefunktion gemäß dem Industriestandard über durch Kommata getrennte, aufgelistete Berechtigungen implementiert. Beim Walkthrough durch den Entwickler*innen-Login-Flow nach Einführung der Login-Experience im Jahr 2014 wurden hingegen elf Dialogfenster und 17 Schritte identifiziert, die bestimmte Aktionen erforderten (z. B. Klicken, Auswählen, Eingeben, Hochladen, Bestätigen), um die gleiche Berechtigungsanfrage zu stellen wie zuvor durch mehrere Code-Zeilen.

Die GUI-fizierung von Programmierpraktiken und die Einführung einer detaillierten Schrittabfolge zur Anforderung von Berechtigungen, die weit über die Anforderungen des OAuth-Standards hinausreichen, strukturiert den Handlungsraum kontinuierlich durch Grammatisierung um. Dieser Eingriff ist signifikant: Er ermöglicht die plattformseitige Regulierung flexibler, gestaltbarer und

41 Spehar: The New Facebook Login and Graph API 2.0.

42 Um die Walkthroughs historisch einzuordnen, habe ich sie durch die Analyse von Tutorial-Videos ergänzt, die auf der Facebook-Plattform für Entwickler sowie der Videoplattform YouTube aus den jeweiligen Jahren verfügbar sind.

43 Philip E. Agre: Surveillance and Capture: Two Models of Privacy, in: *The Information Society*, Bd. 10, Nr. 2, 1994, 101–127, hier 102, doi.org/10.1080/01972243.1994.9960162.

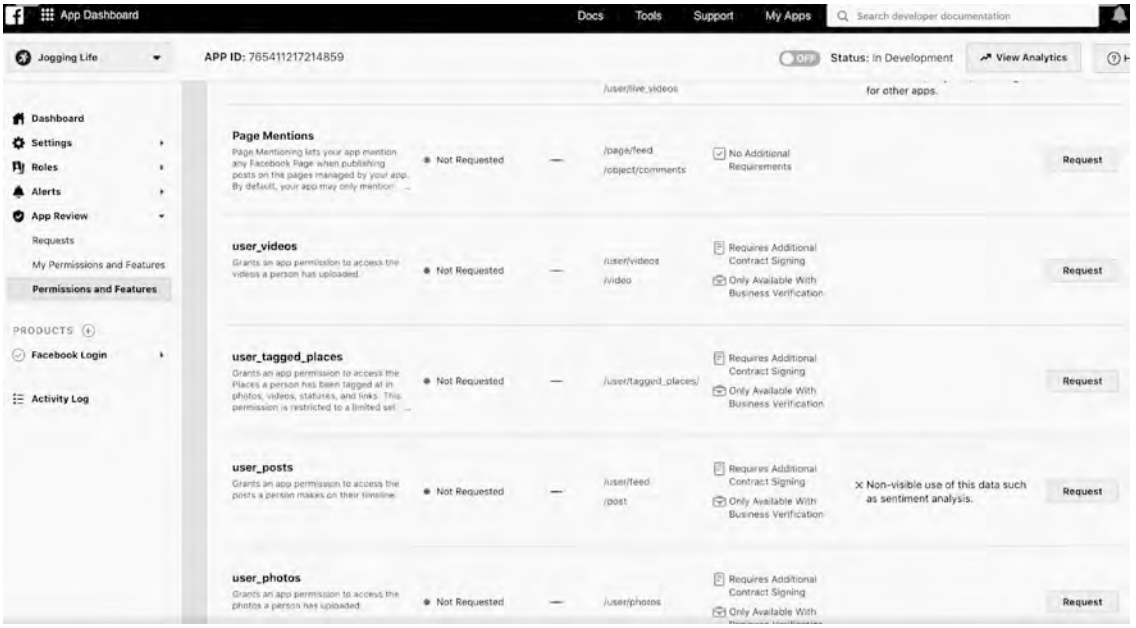

Abb. 2 **Entwickler*innen-User-Flow. Auswahlprozess der von einer Drittanbieter*innen-App angeforderten Berechtigungen**

ergebnisoffener Programmierpraktiken sowie ihres generativen Potenzials. Der diachrone Login-Flow aus der Perspektive der Entwickler*innen führt somit vor Augen, wie die Bequemlichkeitslogik des API-Zugriffs durch eine Form der Einhegung umgesetzt und im praktischen Vollzug erreicht wird.

Eingebettete User Flows. Durch eine ort- und zeitbasierte Untersuchung der Login-Experience durch eingebettete User Flows werden weitere Abweichungen vom Standard bemerkbar. Um weitere situative Berechtigungsanfragen sichtbar zu machen, wurde die primäre Methode zur Anforderung von Berechtigungen – der Login-Prozess – neu verortet, indem sie um zusätzliche, in Aktivitäten eingebettete Datenschutzabläufe erweitert wurde. Gemäß Industriestandard OAuth 2.0 sollen Berechtigungen bei der Erstanmeldung der Nutzer*innen in einer Drittanbieter*innen-App angefordert werden. Diese Berechtigungen werden auf dem Zustimmungsbildschirm angezeigt, dem zweiten hier analysierten Mechanismus. Im Rahmen der Untersuchung des Verstoßes gegen den Datenschutz durch das Unternehmen konzentrierte sich die Überprüfung der Datenschutzarchitektur von Facebook durch die FTC daher insbesondere auf die Anzeige der Berechtigungen auf dem Zustimmungsbildschirm, der den Benutzer*innen während des Anmeldeprozesses angezeigt wird. Der Zustimmungsbildschirm ist aus Sicht der FTC wichtig, da die Zustimmung der Nutzer*innen gemäß den gesetzlichen Rahmenbedingungen erforderlich ist, um jede API-basierte Datentransaktion wirksam zu legitimieren.[44]

Die Analyse der Login-Experience zeigt jedoch, dass die erste Anmeldung nach dem Update zwar weiterhin der primäre Zeitpunkt für die Berechtigungs-

44 Vgl. Richard Warner, Robert Sloan: Beyond Notice and Choice. Privacy, Norms, and Consent, in: *J. High Tech. L.* [Website des Chicago-Kent College of Law am Illinois Institute of Technology], Januar 2013, scholarship.kentlaw.iit.edu/fac_schol/568 (14.12.2025); Daniel L. Solove: Introduction. Privacy Self-Management and the Consent Dilemma, in: *Harvard Law Review*, Nr. 126, Nr. 7, 2013, 1880–1903, harvardlawreview.org/wp-content/uploads/2013/05/vol126_solove.pdf (15.12.2025); ders., Woodrow Hartzog: The FTC and the New Common Law of Privacy, in: *Columbia Law Review*, Nr. 114, 2014, 583–676, doi.org/10.2139/ssrn.2312913.

anfrage ist, die Plattform jedoch zusätzliche Empfehlungen zur Optimierung dieser Anfragen herausgibt, die über die Spezifikationen des Standards hinausgehen. Diese Best-Practice-Empfehlungen für Entwickler*innen zielen darauf ab, die Anzahl der auf dem ersten Login-Zustimmungsbildschirm angezeigten Berechtigungen zu minimieren. Facebook erklärt, dass die Anzeige vieler Berechtigungen als «suspicious» angesehen werden könne, was zu Frustration und einer geringeren Motivation führe, Informationen mit der Drittanbieter*innen-App zu teilen.[45] Laut einer Unternehmensstudie von Facebook verzeichnen Apps, die mehr als vier Berechtigungen anfordern, einen «significant» Rückgang ihrer Konversionsrate bei abgeschlossenen Anmeldungen.[46] Stattdessen wird ein als komfortabel erachteter Datenschutz in diesem Fall durch die Einbettung zusätzlicher Berechtigungsanforderungsabläufe in die technischen Einstellungen alltäglicher Aktivitäten erreicht, wodurch eine gehäufte Anzeige von erforderlichen Berechtigungen während der Anmeldung vermieden wird.[47] Zusätzlich zum Login-User-Flow verzweigen sich diese eher routinehaften und situativen Abläufe zu mehreren Pfaden, die jeweils unterschiedliche Aktivitäten darstellen, denen Nutzer*innen nachgehen können. Entlang dieser in alltäglichen Aktivitäten eingebetteten User Flows können Nutzer*innen auf den Autorisierungsdialog stoßen, wenn sie beispielsweise eine Aktivität aus einer Drittanbieter*innen-App auf Facebook posten oder nach Freund*innen suchen, die dieselbe Drittanbieter*innen-App verwenden.

Die Einbettung von Datenschutzanforderungen in die Routinen des digitalen Alltags kann aus der «socio-material situational embeddedness» dieser User Flows heraus freigelegt werden.[48] Hier kann der *desginerly*-User-Flow eingesetzt werden, um einen Teil der Plattformpolitik von Facebook nachzuvollziehen und die Login-Experience als zentrales (aber für Nutzende kaum bemerkbares) Moment der Aushandlung und Ausgestaltung digitaler Privatheit einer Überprüfung zu unterziehen. Auf der soziotechnischen Ebene wird die Bequemlichkeitslogik in die API-Architekturen implementiert, indem der Datenschutz in zahlreiche Berechtigungsanforderungen segmentiert und in granulare Datenendpunkte zerlegt wird. So wird das Recht auf Datenschutz in die hochgradig routinisierten, habitualisierten Praktiken des digitalen Alltags eingebettet. Den Überlegungen der Ethikerin Elizabeth Edenberg und der Computerhistorikerin Meg Leta Jones zufolge führt die Bewertung des digitalen Datenschutzes auf der Grundlage situativer, individueller Entscheidungen dazu, dass Nutzer*innen dazu neigen, ihren «narrow self-interests» zu folgen und dabei eher bereit sind, Kompromisse für eine unmittelbarere Befriedigung einzugehen.[49] Die Einbettung technischer Datenschutzarchitekturen in alltägliche Aktivitäten kann daher als strategische Verknüpfung von Zugriffsmanagement und Affekt angesehen werden, wobei die unmittelbaren Interessen, die mit dem Teilen, Suchen oder Einrichten einer App verbunden sind, den bewussten Entscheidungsprozess umgehen, den eine aufgeklärte Zustimmung üblicherweise erfordert.

45 Facebook: Permissions with Facebook Login [Beitrag auf Unternehmensblog], *Facebook for Developers*, o. D., archiviert 21.5.2015, *web.archive.org/web/20150521221227/https://developers.facebook.com/docs/facebook-login/permissions/v2.3* (14.12.2025).

46 Ebd.

47 Meta: Facebook Login Best Practices [Beitrag auf Unternehmensblog], *Meta for Developers*, o. D., *developers.facebook.com/docs/facebook-login/best-practices* (14.12.2025).

48 Dieter u. a.: Multi-Situated App Studies.

49 Elizabeth Edenberg, Meg Leta Jones: Analyzing the Legal Roots and Moral Core of Digital Consent, in: *New Media & Society*, Bd. 21, Nr. 8, 2019, 1804–1823, zit. n. Online-Version 1–20, hier 12, *doi.org/10.1177/1461444819831321*.

Der Walkthrough eingebetteter User Flows legt einen komplexen Mechanismus offen. Durch den Einsatz fluider, bedienfreundlicher Datenschutzarchitekturen werden gezielt Öffnungen geschaffen, um die Forderungen nach datenschutzfreundlicheren und datenarmen technischen Systemen zu umgehen. Die Fragmentierung des Datenschutzes in aktivitätsspezifische Zustimmungsanfragen ermöglicht es der Plattform, sich externem Druck anzupassen und zugleich ihre dominante Position auf dem Markt weiter auszubauen. Öffnungen sind für Plattformbetreiber, deren Geschäftsmodelle darauf ausgerichtet sind, Wert aus Datenströmen zu schöpfen, von entscheidender Bedeutung. Die Ökonomin Shoshana Zuboff kritisiert, dass digitale Plattformen durch Erfassung, Analyse und algorithmische Musterbildung einen «behavioural surplus» aus den digitalen Spuren des Alltags extrahieren, da die Produktion und Verarbeitung von Daten weit über das hinausgeht, was für die Bereitstellung bestimmter Dienste erforderlich ist.[50]

Mehrseitige User Flows. Die Bequemlichkeitslogik erzeugt eine starke Wiedererkennbarkeit einer vertrauten Datenschutzkonfiguration (wie sie etwa im OAuth-Protokoll oder im gesetzlichen Rahmen definiert ist), indem sie alle zentralen Mechanismen als scheinbar nachvollziehbar und unmittelbar nutzbar präsentiert. Eine Gegenüberstellung der Login-Prozesse aus der Sicht der verschiedenen Plattform Stakeholder kann genutzt werden, um derartige Verschleierungsstrategien der Plattform aufzudecken und ihnen kritisch zu begegnen. Die Analyse des Login-Prozesses aus der Perspektive unterschiedlicher Rollen (*user persona*) – Entwickler*innen, Nutzer*innen und FTC-Mitarbeiter*innen – zeigt, wie die Personalisierung der Login-User-Flows auf jeder Seite im praktischen Vollzug dazu beiträgt, die Login-Experience als eine sinnvolle Form des Datenschutzes zu stabilisieren. Der Entwickler*innen-Flow wird für die Berechtigungsanfrage vereinfacht, während der Endnutzer*innen-Flow auf die Erteilung von Berechtigungen zugeschnitten ist. Der FTC-Flow[51] hingegen ist so gestaltet, dass er den Ausdruck einer informierten Einwilligung (*informed consent*) auf dem Zustimmungsbildschirm erkennen lässt. Jeder Ablauf ist genauestens darauf ausgelegt, nur solche Datenschutzaspekte zu akzentuieren, die speziell auf die Bedürfnisse der jeweiligen Seite zugeschnitten sind. Da es keine Mechanismen zur direkten Lösung von Datenschutzkonflikten zwischen Nutzer*innen und Drittentwickler*innen gibt, erlaubt der nutzer*innenzentrierte Ansatz es dem Plattformbetreiber, die Art und Weise, wie Konflikte ausgehandelt werden, zu verbergen und die Kompromisse zu verschleiern, die man für die Interessengruppen der Plattform eingeht.

Die auf unterschiedlichen Perspektiven auf die Plattform beruhende Prüfung der historisch verorteten und situativ eingebetteten Login-Flows macht die Bequemlichkeitslogik bedienfreundlicher Interfaces als ein Konzept der stetigen Verwaltung von Zielkonflikten zwischen den widersprüchlichen Interessen

50 Shoshana Zuboff: *The Age of Surveillance Capitalism. The Fight for a Human Future at the New Frontier of Power*, New York 2019.

51 Der Login-Flow aus der Perspektive der *user persona* ‹FTC-Mitarbeiter*in›.

unterschiedlicher Nutzer*innengruppen einer Plattform sichtbar. Während die Grammatisierung offener und explorativer Programmierungspraktiken systematisch eine kontinuierliche Einbindung von Entwickler*innen in die Verdatungspraktiken der Graph API ermöglicht, schafft die dezentrale Streuung und interessengruppenspezifische Personalisierung des Nutzungsverhaltens Öffnungen und Spielräume, durch die die Plattform ihr Macht- und Kontrollsystem kontinuierlich modulieren und ausbauen kann. Auf diese Weise wirkt der Raum der Gestaltungsmöglichkeiten in Software zugleich generativ und einschränkend.

Fazit

Digitaler Datenschutz ist ein zentraler Mechanismus, um Plattformen einer gesetzlichen Kontrolle zu unterwerfen; zugleich löst er öffentliche Kritik und wissenschaftliche Untersuchungen zu den Datenpraktiken von Plattformen aus. Vor diesem Hintergrund ist die Hinwendung von Facebook zum bedienfreundlichen Datenschutz besonders zynisch, da das Versprechen eines verbesserten Datenschutzes mit einer Neuausgestaltung einhergeht, die bestehende Datenzugriffslogiken in der Praxis weiter intensiviert. Während digitaler Datenschutz für Regulierungsbehörden ein auszuübendes Recht darstellt, gestalten Plattformen den Datenschutz habituell und alltäglich. Schnell, mühelos und routiniert ausgeführt, tritt der Datenschutz in den Hintergrund und fügt sich subtil in die technischen und sozialen Systeme des Alltags ein. Obwohl das User Experience Design zu einem vorherrschenden Modell der Governance und Kontrolle geworden ist, hat die Medienwissenschaft bislang kaum untersucht, wie der Paradigmenwechsel im API-Design die Bedingungen des datafizierten Webs neu strukturiert. Ein zentrales Anliegen dieses Beitrags war es daher, zu untersuchen, wie Datenschutz mit einer Bequemlichkeitslogik vereint wird und was dies über bedienfreundliche Formen der Governance innerhalb datenintensiver digitaler Infrastrukturen aussagt.

Um dies an einem konkreten, populären und zugleich nicht leicht zu erschließenden Beispiel zu erörtern, hat der Beitrag die praktische Umsetzung von Datenschutz-Anforderungen in bedienfreundlichen API-Architekturen anhand von Facebooks Login-Experience untersucht. Anhand von *designerly*-User-Flows hat der Beitrag aufgezeigt,[52] wie durch User Experience Design erzeugte APIs den digitalen Alltag strukturieren. Diverse Walkthroughs zur Neuverortung bedienfreundlicher Formen von Governance haben offengelegt, wie das Versprechen eines schnell und bequem umsetzbaren Datenschutzes mit Praktiken der Verschleierung seitens der Plattform einhergeht. Diese Praktiken modulieren die infrastrukturellen Bedingungen, indem sie umgestalten und selektive Perspektiven erzeugen, die die Komplexität der Login-Experience kaschieren, anstatt Risiken zu reduzieren oder den Schutz nicht-öffentlicher Informationen zu verbessern. Entscheidende Merkmale der Bequemlichkeitslogik in datenintensiven Plattformökonomien sind ihr

52 In Anlehnung an Dieter, Tkacz: The Patterning of Finance/Security.

Potenzial zur Hervorbringung wahrnehmbarer und programmierbarer Handlungsoptionen, ihre Anpassungsfähigkeit an äußere Spannungen und die Möglichkeit, Komplexität zu verbergen und zugleich fragmentiert und diffus zu operieren. Statt durch klare Regeln und standardisierte Praktiken regulieren Plattformen durch permanente Modulationen, die zugleich unterstützend und lenkend, ermöglichend und steuernd, öffnend und einschränkend wirken. Während das User Experience Design reibungslose Abläufe verspricht, wird Bedienfreundlichkeit im Fall der Login-Experience durch die gezielte Einführung zusätzlicher Reibungen in Form von GUIs, Schritten, Klicks, dezentralen Flows, gestreuten Datenpunkten sowie selektivem Wissen erreicht. Die Wirksamkeit eines Datenschutzes, der durch eingeübtes Klicken, Wischen und Flows in hohem Maße habitualisiert wird, um die Produktion, Analyse oder Zirkulation von Datenflüssen zu regulieren, wird so in der alltäglichen Praxis weitgehend ausgehebelt. So kann Datenschutz formal implementiert werden, ohne wirkmächtig zu werden.

Förderhinweis: gefördert durch die Deutsche Forschungsgemeinschaft (DFG) – Projektnummer 262513311 – SFB 1187.