🔎 Tiefenrecherche zu W Social, ATProto und der Behauptung lebenslanger ID-gebundener Blocklisten

🧭 Executive Summary

Die belastbarsten Primärquellen ergeben ein klar gegliedertes Bild: Das offizielle Material von belegt, dass die Plattform auf dem AT Protocol[1] aufbaut, dass für schreibende Nutzung eine verifizierte menschliche Identität verlangt wird und dass bei der Registrierung Daten aus der App W Identity[2] an W Social übermittelt werden, nämlich eine W-Identity-UUID, Passland und Geburtsjahr. Belegt ist ebenfalls, dass Standardfunktionen aus dem Bluesky-/ATProto-Ökosystem wie Blocks, Modlists, Labels und Labeler existieren. Nicht belegt ist hingegen, dass Blocklisten oder Blocks protokollseitig oder in öffentlich dokumentierter W-Social-Implementierung „lebenslang“ an eine persoenliche Ausweisverifikation gekoppelt waeren. [3]

Die Kernbehauptung des X-Users zerfaellt deshalb in drei Teile, die man sauber trennen muss. Erstens: Blocks und Blocklisten sind im Bluesky-/ATProto-Stack real und technisch relevant. Das ist klar belegt. Zweitens: Diese Blocks sind im Protokoll an Accounts bzw. DIDs gebunden, nicht an buergerliche Identitaeten. Auch das ist klar belegt. Drittens: Eine lebenslange, personenbezogene Verknuepfung von Blockstatus mit Ausweis- oder eID-Daten ist weder aus den offiziellen ATProto-Spezifikationen noch aus den frei zugaenglichen W-Social-Pflichtdokumenten ableitbar. Dieser Teil der Behauptung ist daher nicht belegt und auf Protokollebene sogar klar fehladressiert. [4]

Gleichzeitig bleibt ein realer, aber enger begrenzter Risikokern uebrig: Weil W Social nach eigener Datenschutzerklaerung eine W-Identity-UUID entgegennimmt und zugleich Moderation von „illegal or harmful content“ vorsieht, waere eine nicht-oeffentliche Betreiberlogik technisch denkbar, die mehrere Accounts derselben verifizierten Person miteinander korreliert oder Moderationsentscheidungen kontenuebergreifend vollzieht. Fuer eine solche UUID-gestuetzte Personenbindung gibt es derzeit jedoch keine primaere Evidenz in den oeffentlich zugaenglichen Artefakten. Das ist also ein plausibles Risiko, aber kein nachgewiesener Ist-Zustand. [5]

Mein Gesamturteil lautet deshalb: Die Warnung ist in dem Punkt zutreffend, dass W Social eine echte Identitaetsverifikation als Zugangshuerde fuer aktive Teilnahme vorsieht und dass ATProto/Bluesky oeffentliche Blocks und Moderationsmechanismen kennt. Sie ist aber irrefuehrend bis ueberzogen, soweit sie behauptet, das Protokoll sei darauf ausgelegt, Blocks „lebenslang“ an persoenliche Ausweisverifikation zu koppeln und Menschen dadurch technisch unumkehrbar „vom Diskurs“ auszuschliessen. Genau dieser starke Schluss ist nach heutigem Primaermaterial nicht gedeckt. [6]

Claim-Matrix

Sub-Claim	Primaerquelle(n)	Technischer Befund	Klassifikation	Begruendung	Restunsicherheit
Blocks und Blocklisten sind im Bluesky-/ATProto-Stack vorhanden.	[7]	Ja. User-Blocks, List-Blocks, Moderationslisten und Labeler sind Standardbausteine.	**1**	Bluesky dokumentiert `app.bsky.graph.block`, `app.bsky.graph.listblock`, Modlists und Labeler explizit.	Gering.
Blocks sind an Accounts bzw. DIDs gebunden, nicht an Handles.	[8]	Ja. Der Block-Record verwendet DIDs; Handles sind nur mutable Benutzernamen.	**1**	Die Block-Tutorials nennen DIDs als `repo` und `subject`; die Spezifikation definiert DIDs als primaere Account-Identifier und Handles als mutable.	Gering.
Das AT-Protokoll sei so „vorgesehen“, dass Blocks lebenslang an persoenliche ID-Verifikation gekoppelt werden.	[9]	Nein. Das Protokoll modelliert Account-Identitaet ueber DID/Handle/PDS, nicht ueber staatliche Identitaetspruefung.	**2**	In den offiziellen Spezifikationen ist keine Ausweis-, eID- oder KYC-Schicht als Protokollbestandteil vorgesehen. W Social fuegt Identitaetspruefung allenfalls als Betreiber-Overlay hinzu.	Gering bis mittel, weil proprietaere Operator-Overlays natuerlich moeglich bleiben.
W Social verlangt verifizierte menschliche Identitaet fuer aktive Konten.	[10]	Ja.	**1**	Die Datenschutzerklaerung sagt, jedes Konto sei mit einer „verified human identity“ zu verknuepfen; Deutschlandfunk berichtet ueber Ausweisverifikation fuer Nutzer.	Gering.

Sub-Claim	Primaerquelle(n)	Technischer Befund	Klassifikation	Begruendung	Restunsicherheit
W Social beweist oeffentlich „one human, one account“.	[10]	Nur teilweise.	**3**	Belegt ist „each account be associated with a verified human identity“. Nicht belegt ist die staerkere Aussage, dass eine Person nur ein einziges Konto halten darf oder technisch nicht mehrere Konten bekommen kann.	Mittel.
W Social uebernimmt bei Signup eine stabile Identitaetskennziffer.	[5]	Ja, eine W-Identity-UUID wird uebermittelt; die App fungiert als digitale Identitaets-App.	**1**	Die Datenschutzerklaerung nennt die UUID ausdruecklich; der offizielle App-Store-Eintrag beschreibt W Identity als e-identification-App.	Gering.
Blocks oder Moderationsstatus werden bei W Social nachweislich an diese UUID oder reale Ausweisdaten gekoppelt.	[5]	Hierfuer gibt es derzeit keine primaere Evidenz.	**5**	Die offiziellen Texte sagen, welche Identitaetsdaten fliessen. Sie sagen nicht, dass Block- oder Moderationsstatus an UUID, Passland oder Geburtsjahr gebunden werden.	Hoch, weil die relevante Backend-Logik nicht oeffentlich dokumentiert ist.
Die behauptete Koppelung ist dennoch ein plausibles reales Risiko.	[5]	Ja, technisch plausibel.	**4**	Wer eine plattforminterne UUID fuer jeden verifizierten Nutzer besitzt, koennte daraus konto-uebergreifende Moderation	Mittel.

Sub-Claim	Primaerquelle(n)	Technischer Befund	Klassifikation	Begruendung	Restunsicherheit
				ableiten. Dass dies geschieht, ist aber nicht belegt.	
„For life“: Ein Block ist in Bluesky/ATProto irreversibel oder lebenslang.	[11]	Nein. Blocks koennen geloescht werden; auch Account-Status sind teils revertierbar.	**2**	Unblocking geschieht durch Loeschen des Block-Records; auch takedown/deleted-Zustaende sind in der Spezifikation nicht metaphysisch irreversibel.	Gering.
Ein Block kann fuer dasselbe Konto ueber Handle- oder PDS-Wechsel fortwirken.	[12]	Ja.	**1**	Weil DIDs persistent sind und Handles/PDS wechseln koennen, bleibt kontobezogene Moderation fuer dieselbe DID prinzipiell erhalten.	Gering.
„Vom Diskurs ausgeschlossen“ im Sinn totaler, netzwerkweiter, lebenslanger Unsichtbarkeit folgt aus dem Protokoll.	[13]	Nein, so stark nicht.	**3**	Blocks verhindern Interaktion und Sichtbarkeit in protokollkonformen Clients. Oeffentliche Inhalte bleiben aber weiterhin ausserhalb des eingeloggten Kontexts oder ueber andere Accounts sichtbar.	Mittel, weil AppViews/Relay-Politiken variieren koennen.

Legende der Klassifikationen: 1 = klar belegt; 2 = klar widersprochen; 3 = teilweise belegt, aber ueberzogen; 4 = plausibles reales Risiko, aber nicht nachgewiesen; 5 = derzeit nicht entscheidbar. [14]

Audit der oeffentlichen Artefakte von

Die derzeit am klarsten zugaenglichen Primaerartefakte sind die offizielle Datenschutzerklaerung von W Social, der offizielle App-Store-Eintrag fuer die App W Identity und die oeffentlichen ATProto-/Bluesky-Spezifikationen. Aus ihnen laesst sich sicher ableiten, dass W Social AB als schwedische Betreiberin auftritt, dass die Plattform ATProto-basiert ist und dass W Social beim Signup eine externe Identitaetspruefung ueber W Identity einbindet. W Social erhaelt dabei nach eigener Auskunft die W-Identity-UUID, das Passland und das Geburtsjahr; ferner erhebt W Social standardmaessig Social-Graph-Daten einschliesslich Follow-, Mute- und Blocklisten. Zudem nennt die Datenschutzerklaerung Moderation von „illegal or harmful content“ als Verarbeitungszweck. [15]

Ein weiteres, wenn auch schwaches oeffentliches Indiz fuer eine direkte Bluesky-Ableitung ist die Subdomain `stage.wsocial.eu`, die in den Suchergebnissen mit dem Seitentitel „Bluesky“ erscheint. Das beweist noch keinen bestimmten Diff oder Fork-Zustand, stuetzt aber die Einordnung, dass zumindest Teile der Nutzeroberflaeche eng an Bluesky angelehnt sind. Auch die eigene Datenschutzerklaerung von W Social sagt explizit, dass die Plattform auf ATProto basiert und Inhalte von Bluesky integrieren kann. [16]

Was die eigentliche Codebasis angeht, endet die harte Primaerevidenz frueh. Ich kann aus den direkt zugaenglichen Primaerartefakten **nicht** nachweisen, dass oeffentliche W-Social-Repositories eine personengebundene Moderationslogik, UUID-basierte Wiedererkennung derselben Person ueber mehrere Konten oder eine lebenslange Persistenz von Blockstatus implementieren. Die beigefuegte PDF-Voranalyse □filecite□turn0file0□legt zwar per Screenshot nahe, dass ein oeffentliches □url□GitHub□https://github.com□-Org mit Bluesky-abgeleiteten Repositories existiert und dass dort keine offensichtliche eID-/Block-Koppelungslogik sichtbar war; weil diese konkreten Repository-Seiten hier aber nicht unabhaengig als Primaerquellen durchgaengig retrivierbar waren, behandle ich den punktgenauen Repo-Diff-Befund methodisch nur als **provisorisch zusaetzliches** Indiz, nicht als vollstaendig re-auditiertes Ergebnis. [16]

Gerade diese Grenze ist inhaltlich wichtig: Fehlender oeffentlicher Code beweist weder Harmlosigkeit noch das Gegenteil. Er verschiebt die Einordnung solcher Aussagen in die Klassen „plausibles Risiko“ oder „derzeit nicht entscheidbar“. Fuer die starke These des X-Users reicht das, was oeffentlich sichtbar ist, jedenfalls nicht aus. [5]

Protokollanalyse zu Blocks, Identitaet und Portabilitaet

Im offiziellen Design des AT Protocol[1] ist die primaere Kontenidentitaet die DID, nicht der Handle und erst recht nicht eine staatlich verifizierte Person. Die Spezifikation bezeichnet DIDs als persistente Account-Identifier; der Handle ist dagegen nur der menschenlesbare, mutable Name, der an eine DID gebunden wird. Genau daraus folgt: Moderation und Beziehungen, die auf DIDs zielen, koennen fuer dasselbe Konto ueber Handle-Wechsel hinweg fortbestehen. Daraus folgt aber **nicht**, dass dieselbe reale Person ueber neue Konten hinweg automatisch wiedererkannt wird. [17]

Die Blockfunktion selbst ist in Bluesky/ATProto ein oeffentlicher Record im Repo eines Accounts. Das Blocking-Tutorial nennt als repo die DID des blockierenden Kontos und als `subject` die DID des blockierten Kontos. Das Bluesky-Blog erklaert dazu ausdruecklich, dass Blocks oeffentlich und enumerierbar sind, weil alle Server im Netz von ihnen wissen muessen, um sie durchzusetzen. Das ist also eine konten- und netzkonforme Durchsetzungsarchitektur, keine Ausweisarchitektur. [18]

Ebenso wichtig ist, was Blocks **nicht** tun. Sie sind nicht irreversibel; unblocking geschieht durch Loeschen des Block-Records. Sie aendern auch nicht das Repo des Geblockten, loeschen dessen alte Replies nicht und verhindern nicht, dass oeffentliche Inhalte ausgeloggt oder ueber ein anderes Konto gelesen werden. Blocks reduzieren Interaktion und Sichtbarkeit im protokollkonformen Oekosystem; sie erzeugen aber keine absolute, lebenslange Tilgung einer Person aus dem Diskurs. [19]

Auch die breitere Moderationsarchitektur von Bluesky/ATProto spricht gegen den simplen Kurzschluss des X-Posts. Die offizielle Moderationsdokumentation trennt mehrere Schichten: Netz-Takedowns, Labels durch Moderationsdienste sowie Nutzerkontrollen wie Mutes und Blocks. Labeler sind normale atproto-Accounts mit eigener DID-Konfiguration und publizieren Moderationspolitik separat. Das bedeutet: „Aus dem Diskurs ausgeschlossen“ kann technisch sehr verschiedene Formen meinen — vom privaten User-Block bis zum AppView-Takedown. Diese Schichten darf man nicht unbesehen zusammenschieben. [20]

Schliesslich ist ATProto portabel. Die Accounts-Spezifikation erklaert ausdruecklich PDS-Migrationen, die Persistenz der DID sowie Status wie `deactivated`, `suspended`, `takendown` und `deleted`. Diese Status sind teils temporaer, teils langfristig gemeint, aber nicht als metaphysisch unumkehrbarer „fuer immer“-Mechanismus beschrieben. Ein protocol-native Lebenslangkeitsnarrativ ist deshalb falsch. Was bleibt, ist hoechstens eine Kontinuitaet derselben DID-Identitaet, solange derselbe Account fortgefuehrt wird. [21]

⚠ W-Social-spezifische Risikoanalyse

Der eigentliche Risikopunkt bei W Social liegt **nicht** im ATProto-Design selbst, sondern in der identitaetspruefenden Betreiber-Overlay-Schicht. W Social bestaetigt, dass fuer ein Konto eine verifizierte menschliche Identitaet erforderlich ist und dass W Social vom W-Identity-System eine UUID, Passland und Geburtsjahr entgegennimmt. Diese Datenuebernahme schafft zumindest einen technisch geeigneten Anker, um spaeter konto- oder personenuebergreifende Entscheidungen zu treffen. Ohne eine solche Kennziffer waere plattformweite Personenkorrelation schwerer; mit ihr wird sie prinzipiell machbar. [5]

Aber: Aus Machbarkeit folgt noch keine Implementierung. In den zugaenglichen W-Social-Primärtexten findet sich **keine** Aussage, dass dieselbe W-Identity-UUID fuer Moderation, Wiedererkennung geloeschter Nutzer, Cross-Account-Bans oder lebenslange Blockpersistenz verwendet wird. Die Datenschutzerklaerung nennt die UUID im Zusammenhang mit Kontopruefung und Kontoerstellung; sie nennt ausserdem allgemeine Moderation. Sie verbindet beides jedoch nicht explizit miteinander. Genau deshalb darf

man aus dem blossen Vorhandensein der UUID keine bewiesene „lifetime ban“-Architektur konstruieren. [22]

Realistische Gefahrenszenarien bleiben dennoch uebrig. Ein Betreiber koennte hinter den Kulissen einen Identity-Graph fuehren, in dem mehrere Konten derselben verifizierten Person zusammenlaufen. Er koennte Wiederanmeldungen derselben Person erkennen, globale Sperren ueber mehrere Konten anwenden, Discovery drosseln oder AppView-seitig Sichtbarkeit reduzieren, ohne dies im offenen Protocol-Layer abzubilden. All das waere **technisch moeglich**, sofern W Social die UUID dauerhaft und operationell nutzbar haelt oder ein paralleles proprietaeres Moderationssystem betreibt. Fuer keinen dieser Punkte gibt es derzeit aber Primaerevidenz im oeffentlich zugaenglichen Material. [5]

Ebenso wichtig ist der Gegenzug: Selbst wenn W Social „one verified human per account“ ernst meint, folgt daraus noch nicht „one human, one account“. Die Satzstruktur in der Datenschutzerklaerung ist asymmetrisch: Jedes Konto muss mit verifizierter menschlicher Identitaet verbunden sein; nicht gesagt wird, dass jede menschliche Identitaet nur genau ein Konto besitzen kann. Gerade an diesem Punkt ist der X-Post deutlich staerker als die derzeit oeffentlich bestaetigte Tatsachenlage. [22]

Kurz: Die echte Gefahr liegt nicht in einer angeblich bereits bewiesenen Protokollfunktion, sondern in moeglicher proprietaerer Betreiberlogik auf Basis einer verifizierenden UUID. Diese Gefahr ist real genug, um kritische Transparenzforderungen zu rechtfertigen. Sie ist aber im Moment nicht dokumentarisch so belegt, dass man sie als feststehende Implementierung ausgeben duerfte. [5]

📜 Schlussurteil und offene Fragen

Was **unterstuetzt** ist: W Social baut auf ATProto auf; W Social verlangt fuer aktive Teilnahme verifizierte menschliche Identitaet; W Social erhaelt bei der Registrierung eine W-Identity-UUID, Passland und Geburtsjahr; Bluesky/ATProto kennt oeffentliche Blocks, Modlists und mehrschichtige Moderation; Blocks sind DID-/accountgebunden und koennen deshalb fuer denselben Account ueber Handle-Wechsel hinaus wirksam bleiben. [23]

Was **widersprochen** ist: Dass das Bluesky-basierte AT-Protokoll selbst darauf angelegt sei, Blocks „lebenslang“ an persoenliche Ausweisverifikation zu koppeln. Das ist mit den offiziellen Spezifikationen nicht vereinbar. Ebenso ist die Vorstellung eines blocktechnisch irreversiblen „for life“ im engen technischen Sinn falsch, weil Block-Records geloescht werden koennen und weil das Protokoll keine eingeborene Person-ID-Schicht kennt. [24]

Was **plausibles Risiko** bleibt: Wenn W Social die uebermittelte W-Identity-UUID dauerhaft betriebsintern nutzt, koennte der Betreiber mehrere Konten derselben Person korrelieren und Moderation konto- oder personenuebergreifend vollziehen. Das waere ein echter Freiheits- und Datenschutzhebel. Oeffentlich nachgewiesen ist diese Umsetzung derzeit aber nicht. [5]

Was **derzeit nicht entscheidbar** ist: Ob eine proprietaere Backend-Logik existiert, die Block- oder Moderationsstatus an die W-Identity-UUID, an Ausweisdaten, an biometrische Verifikation oder an eine interne Personenkennung bindet; ob Wiederanmeldungen derselben Person erkannt und sanktioniert werden; ob „one human, one account“ wirklich technisch erzwungen wird; und ob globale, appviewweite oder relayweite Sichtbarkeitsbeschraenkungen fuer verifizierte Personen hinterlegt sind. Hier endet die primaere Evidenz. [25]

Mein direktes Gesamturteil lautet daher: **Die Warnung ist im Kern nicht fundamental falsch, aber in ihrer staerksten Form irrefuehrend.** Zutreffend ist, dass W Social eine identitaetsgestuetzte Zugangsschicht plant und dass der verwendete Protocol-Stack oeffentliche Blocks und Moderationsinstrumente kennt. **Nicht** belegt ist der behauptete Schluss, dass Kritik einmalig zu personengebundener, lebenslanger Ausgrenzung durch blocklistenartige Mechanismen fuehre. Der sauberste Befund ist: **teilweise wahr im Ausgangspunkt, aber deutlich ueberzogen in der Schlussfolgerung; fuer die eigentliche Personenbindung im Backend derzeit nicht entscheidbar.** [6]

Die wichtigsten zusaetzlichen Artefakte fuer eine echte Endbeurteilung waeren: die private Backend-Logik fuer Signup und Moderation, eine formelle Moderationsrichtlinie, technische Dokumentation zu W Identity und zur Bedeutung der UUID, die API-Dokumentation zwischen W Identity und W Social, ein oeffentliches Datenmodell oder Schema fuer Sperr- und Moderationsentscheidungen sowie die realen mobilen App-Binaries mit analysierbaren Netzwerkaufrufen. Ohne diese Artefakte bleibt jede Behauptung ueber lebenslange personenbezogene Blockpersistenz entweder Spekulation oder blosses Risikoszenario. [25]

---

[1] [2] [7] [8] [11] [18] [19] [24] https://docs.bsky.app/docs/tutorials/blocking

https://docs.bsky.app/docs/tutorials/blocking

[3] [5] [6] [10] [14] [15] [22] [23] [25] https://wsocial.eu/public/privacy-notice

https://wsocial.eu/public/privacy-notice

[4] [9] [12] [17] https://atproto.com/specs/did

https://atproto.com/specs/did

[13] https://docs.bsky.app/blog/block-implementation

https://docs.bsky.app/blog/block-implementation

[16] https://stage.wsocial.eu/

https://stage.wsocial.eu/

[20] https://docs.bsky.app/docs/advanced-guides/moderation

https://docs.bsky.app/docs/advanced-guides/moderation

[21] https://atproto.com/specs/account

https://atproto.com/specs/account