PUBLIC STACK SCAN

Ibrahim Ishaque

15-10-2024 Hogeschool van Amsterdam

Inhoudsopgave

Inleiding

In deze opdracht ga ik twee veelgebruikte berichtendiensten, Telegram en Signal onderzoeken met behulp van de Public Stack. De Public Stack is een model dat technologie beoordeelt op basis van publieke waarden zoals privacy, veiligheid, toegankelijkheid en transparantie. Het model bestaat uit drie hoofdlagen: de Tech Stack (de technische basis van de technologie), het Designproces (hoe de technologie is ontworpen met de gebruiker in gedachten), en de Foundation (de fundamentele waarden zoals ethiek en governance).

Het doel van deze Public Stack Scan is om te analyseren hoe goed deze twee applicaties voldoen aan publieke waarden. Telegram, hoewel erg populair, krijgt veel kritiek op zijn privacy- en beveiligingsmaatregelen. Signal daarentegen staat bekend om zijn sterke privacybescherming en het gebruik van open-source technologie. Door beide apps te scannen, wil ik inzicht krijgen in welke app beter presteert op het gebied van publieke waarden.

In deze analyse behandel ik:

1. **De Public Stack Scan**: Criteria en indicatoren die ik heb gebruikt om de apps te beoordelen.
2. **Analyse van Telegram**: Een diepgaande beoordeling van Telegram en waar de app tekortschiet.
3. **Analyse van Signal**: Een evaluatie van Signal en waarom het beter scoort op publieke waarden.
4. **Vergelijking van beide applicaties**: Een vergelijking van de resultaten op basis van de Public Stack.
5. **Verbeteringsvoorstellen voor Telegram**: Aanbevelingen om Telegram te verbeteren en meer in lijn te brengen met de publieke waarden van de Public Stack.

Dit document biedt een gedetailleerde beoordeling van hoe goed deze apps voldoen aan de belangrijkste publieke waarden en welke verbeteringen er mogelijk zijn om technologie beter te laten aansluiten op de behoeften van de samenleving.

Uitleg van de Public Stack

De Public Stack biedt een mechanisme om te bepalen of technologie voldoet aan belangrijke kwesties zoals privacy, veiligheid en eerlijkheid. De Public Stack bestaat uit drie onderdelen: de Tech Stack, het Designproces en de Foundation, die samen bepalen hoe goed een app presteert op deze gebieden.

1. **Tech Stack**: Dit gaat over de technische aspecten van de app: hoe veilig is de app, of je gegevens goed beschermd zijn, en hoe goed de technologie werkt. Bijvoorbeeld, worden je berichten versleuteld? En zijn er regelmatig updates om de app veilig te houden?
2. **Designproces**: Dit deel richt zich op het ontwerp van de app en houdt rekening met de diverse mensen die het gebruiken. Is de app gemakkelijk te gebruiken voor iedereen, inclusief mensen met beperkingen? Worden gebruikers serieus genomen, en kunnen ze feedback geven over de app? Dit is belangrijk om ervoor te zorgen dat de app eerlijk is en goed werkt voor verschillende soorten mensen.
3. **Foundation**: Dit gaat over de kernprincipes en waarden van de app. Houdt de app zich aan regels rondom privacy en mensenrechten? Wat gebeurt er met je gegevens, en is er toezicht om te controleren of alles goed gaat? Ook wordt bekeken of de app niet alleen gericht is op winst maken, maar ook het welzijn van de gebruikers in acht neemt.

De Public Stack helpt je te begrijpen of een app goed is voor de samenleving en of het technologie op een verantwoordelijke manier gebruikt. In mijn onderzoek vergelijk ik twee berichtendiensten: Telegram, dat bekendstaat om problemen met privacy en beveiliging, en Signal, dat juist uitblinkt in privacybescherming en transparantie omdat het open-source is. Met deze methode zie je welke apps beter presteren op het gebied van publieke waarden.

Public Stack Scan: Criteria en Indicatoren

Om de apps beter te beoordelen op basis van publieke waarden, gebruik ik een puntensysteem om alles duidelijk en meetbaar te maken. Elke vraag krijgt een score van 1 tot 5, waarbij:

- **1** = slecht (niet aanwezig)
- **5** = uitstekend (heel goed aanwezig)

Dit helpt om te zien welke app beter scoort op punten zoals privacy, veiligheid en toegankelijkheid. Hieronder zijn de vragen die ik gebruik, ingedeeld in de drie lagen van de **Public Stack**: **Tech Stack**, **Designproces**, en **Foundation**.

Categorie	Vraag	Score (1-5)
Tech Stack		
Infrastructuur en apparaten	Is de app bruikbaar op alle apparaten (iOS, Android, PC)?	
	Is de app afhankelijk van speciale hardware?	
Beveiliging	Gebruikt de app versleuteling voor data?	
	Krijg je automatisch beveiligingsupdates?	
	Is tweefactorauthenticatie beschikbaar?	
Openheid en samenwerking	Werkt de app samen met andere apps (open standaarden)?	
	Kun je makkelijk data exporteren?	
	Is de broncode open-source?	
Data en algoritmes	Weet je wat er met je data gebeurt?	
	Zijn de algoritmes van de app duidelijk voor gebruikers?	
Designproces		
Inclusiviteit en participatie	Houdt de app rekening met mensen met een beperking?	
	Konden gebruikers feedback geven tijdens het ontwerpen?	
Toegankelijkheid en gebruiksgemak	Is de app makkelijk te gebruiken?	
	Zijn er handleidingen of hulppagina's beschikbaar?	
Ontwerpmethode	Is de app ontworpen met privacy en toegankelijkheid in gedachten?	
	Kun je makkelijk feedback geven?	
Foundation		
Mensenrechten en publieke waarden	Beschermt de app je privacy goed?	
	Worden je gegevens veilig opgeslagen?	
	Beperkt de app je vrijheid van meningsuiting?	
Governance en toezicht	Is het duidelijk wie verantwoordelijk is voor de app en je data?	
	Worden er onafhankelijke controles uitgevoerd?	
Sociaal-economische impact	Is de app voor iedereen toegankelijk?	
	Is de app milieuvriendelijk?	

Hoe gebruik je de tabel?

1. **Scoor per vraag**: Voor elke vraag geef je een score van 1 tot 5. Bijvoorbeeld, als een app geen tweefactorauthenticatie heeft, zou je daar een 1 kunnen geven. Als het wel beschikbaar en makkelijk te gebruiken is, geef je een 5.
2. **Tel de scores per categorie op**: Nadat je de vragen hebt gescoord, tel je de scores op per categorie. Bijvoorbeeld, de Tech Stack categorie heeft 8 vragen, dus het maximum aantal punten voor die categorie is 40.
3. **Vergelijk de totale scores**: Door de scores van verschillende apps te vergelijken, kun je zien welke app het beste presteert op het gebied van publieke waarden zoals privacy, beveiliging en toegankelijkheid.

Deze tabel maakt de Public Stack Scan visueel en eenvoudig te gebruiken. Hiermee kun je de scores van verschillende apps naast elkaar zetten en snel zien welke het beste scoort op basis van jouw criteria.

Analyse van Applicatie 1 (lage score op publieke waarden)

Korte beschrijving van de applicatie

Telegram is een populaire berichtendienst die wereldwijd veel gebruikers heeft. Het staat bekend om snelle communicatie en een eenvoudig te gebruiken interface, maar er zijn ernstige zorgen over hoe Telegram omgaat met beveiliging en privacy.

Tech Stack

Infrastructuur en apparaten

- **Bruikbaarheid op alle apparaten:** Telegram is beschikbaar op meerdere platforms, zoals iOS, Android, en PC, wat de toegankelijkheid ten goede komt. **Score: 5/5**.

Beveiliging

- **Versleuteling:** Telegram gebruikt zijn eigen encryptieprotocol, **MTProto**, wat minder transparant is en kritisch wordt bekeken door experts. Het grootste probleem is dat **standaardberichten niet end-to-end versleuteld** zijn. Hierdoor worden berichten alleen versleuteld tijdens de overdracht naar de servers van Telegram, maar niet van gebruiker tot gebruiker. Alleen **geheime chats** bieden volledige end-to-end encryptie **Score: 2/5** (Page, 2024).
- **Beveiligingsupdates:** Telegram biedt regelmatige beveiligingsupdates, maar de standaardbeveiliging schiet tekort zonder end-to-end encryptie voor alle berichten. **Score: 4/5**.
- **Tweefactorauthenticatie:** Tweefactorauthenticatie is beschikbaar, wat de beveiliging van gebruikersaccounts ten goede komt. **Score: 4/5**.

Openheid en interoperabiliteit

- **Samenwerking met andere apps:** Telegram biedt beperkte samenwerking met andere apps en maakt geen gebruik van volledig open standaarden, wat de interoperabiliteit vermindert. **Score: 3/5**.
- **Data exporteren:** Gebruikers hebben beperkte opties om hun gegevens eenvoudig te exporteren naar andere platforms. **Score: 2/5**.
- **Open-source broncode:** Telegram's **clientcode** is open-source, maar de servercode blijft gesloten, wat minder transparantie biedt dan andere open-source applicaties zoals Signal **Score: 3/5** (Bruce Schneier, 2024).

Data en algoritmes

- **Transparantie over data:** Telegram biedt beperkte transparantie over hoe gegevens worden verwerkt, en standaard chats zijn niet volledig beschermd door end-to-end encryptie. **Score: 2/5** (Page, 2024).
- **Transparantie over algoritmes:** Telegram biedt geen volledige duidelijkheid over de algoritmes die worden gebruikt voor gegevensverwerking. **Score: 2/5**.

Designproces

Inclusiviteit en gebruikersparticipatie

- **Toegankelijkheid voor mensen met beperkingen:** Telegram biedt beperkte toegankelijkheidsopties, zoals ondersteuning voor schermlezers, wat problematisch kan zijn voor gebruikers met speciale behoeften. **Score: 2/5**.
- **Gebruikersfeedback tijdens ontwerp:** Telegram lijkt weinig rekening te houden met gebruikersfeedback, vooral wat betreft privacyfuncties **Score: 2/5** (Guneet Kaur, 2024).

Toegankelijkheid en gebruiksgemak

- **Gebruiksvriendelijkheid:** Telegram is eenvoudig te gebruiken, wat een sterk punt is van de app. **Score: 4/5**.
- **Beschikbare handleidingen of hulppagina's:** Telegram biedt basisondersteuning, maar handleidingen zijn niet bijzonder gedetailleerd. **Score: 3/5**.

Ontwerpmethode

- **Privacy en toegankelijkheid in ontwerp:** Telegram houdt niet genoeg rekening met privacy in het standaardontwerp; veel functies moeten handmatig worden ingeschakeld. **Score: 2/5**.
- **Feedbackopties:** Er zijn beperkte mogelijkheden voor gebruikers om gemakkelijk feedback te geven. **Score: 2/5**.

Foundation

Mensenrechten en publieke waarden

- **Privacybescherming volgens de wet:** Telegram voldoet aan basisprivacywetten, maar het gebrek aan end-to-end encryptie voor standaardberichten beperkt de bescherming van gebruikersgegevens **Score: 2/5** (Guneet Kaur, 2024).
- **Veilige opslag van gegevens:** Berichten die niet in geheime chats worden verstuurd, worden opgeslagen op de servers van Telegram, wat een risico vormt **Score: 2/5** (Page, 2024).
- **Censuur en beperking van rechten:** Telegram staat bekend om vrijheid van meningsuiting, maar heeft te maken gehad met druk van overheden om gegevens vrij te geven. **Score: 3/5** (Bruce Schneier, 2024).

Governance en toezicht

- **Verantwoordelijkheid en transparantie:** Telegram biedt beperkte transparantie over wie verantwoordelijk is voor de gegevens van gebruikers. **Score: 2/5**.
- **Onafhankelijke audits:** Telegram heeft geen bewijs geleverd van regelmatige onafhankelijke audits, wat zorgt voor een gebrek aan externe controle. **Score: 2/5**.

Sociaal-economische impact

- **Toegankelijkheid voor iedereen:** Telegram is gratis en voor iedereen toegankelijk, zonder beperkingen op basis van locatie of sociaal-economische status. **Score: 5/5**.
- **Milieuvriendelijkheid:** Er is weinig informatie beschikbaar over de duurzaamheid van Telegram's infrastructuur. **Score: 2/5**.

Conclusie en samenvatting van de scores

Telegram biedt handige functies zoals gebruiksvriendelijkheid en toegang tot meerdere platforms, maar scoort slecht op privacy en beveiliging. Het gebruik van het eigen gesloten MTProto-encryptieprotocol en het gebrek aan standaard end-to-end encryptie maakt de app minder veilig dan alternatieven zoals Signal. Het ontbreken van uitgebreide toegankelijkheidsopties en transparantie beperkt Telegram's prestaties op het gebied van publieke waarden.

Totaalscore:

- **Tech Stack:** 27/40
- **Designproces:** 15/30
- **Foundation:** 18/35

Telegram scoort laag in alle lagen van de Public Stack en laat veel ruimte voor verbeteringen op het gebied van beveiliging, toegankelijkheid en transparantie.

Analyse van Applicatie 2 (hoge score op publieke waarden en open-source licentie)

Korte beschrijving van de applicatie

Signal is een open-source berichtendienst die zich volledig richt op privacy en veiligheid. Het wordt wereldwijd gebruikt door mensen die waarde hechten aan de bescherming van hun persoonlijke communicatie, zoals journalisten, activisten en gebruikers die hun gegevens veilig willen houden. Signal gebruikt volledige end-to-end encryptie voor alle berichten en oproepen, en biedt sterke privacybescherming zonder dat je data wordt opgeslagen op de servers van Signal (Kaul, 2021).

Tech Stack

Infrastructuur en apparaten

- **Bruikbaarheid op alle apparaten:** Signal is beschikbaar op iOS, Android, en desktops, waardoor het op verschillende platforms toegankelijk is. Dit zorgt voor brede beschikbaarheid en maakt het gebruik op meerdere apparaten mogelijk **Score: 5/5** (Mann, 2024).

Beveiliging

- **Versleuteling:** Signal biedt standaard **end-to-end encryptie** voor alle berichten, wat betekent dat zelfs de ontwikkelaars van Signal geen toegang hebben tot de inhoud van de communicatie. Deze sterke encryptie is gebaseerd op het open-source **Signal Protocol**, dat door meerdere beveiligingsexperts wordt geprezen als een van de veiligste protocollen die beschikbaar zijn **Score: 5/5** (Dahan, 2024).
- **Beveiligingsupdates:** Signal ontvangt regelmatige beveiligingsupdates om de app veilig te houden en mogelijke kwetsbaarheden te verhelpen. **Score: 5/5**.
- **Tweefactorauthenticatie:** Hoewel Signal sterke beveiliging biedt via encryptie, ontbreekt een tweefactorauthenticatie (2FA) optie voor het inloggen, wat een gemiste kans is om de beveiliging verder te verbeteren **Score: 4/5** (Mocan, 2024).

Openheid en interoperabiliteit

- **Samenwerking met andere apps:** Signal is volledig onafhankelijk van andere apps en werkt op zichzelf. Het ondersteunt geen externe apps via open standaarden, maar dit komt vooral door de focus op privacybescherming **Score: 3/5** (Kaul, 2021).
- **Data exporteren:** Hoewel Signal een goede privacybescherming biedt, kunnen gebruikers hun gegevens niet eenvoudig exporteren naar andere platformen, wat het voor gebruikers moeilijk maakt om data van Signal naar een ander systeem over te zetten **Score: 3/5** (Mocan, 2024).
- **Open-source broncode:** Signal is volledig open-source, zowel de app als het protocol. Dit betekent dat de broncode door iedereen kan worden gecontroleerd en geverifieerd op veiligheid, wat zorgt voor volledige transparantie **Score: 5/5** (Dahan, 2024)..

Data en algoritmes

- **Transparantie over data:** Signal verzamelt zeer weinig gegevens. Het enige dat vereist is, is je telefoonnummer om je te registreren. Er wordt geen IP-adres, profielinformatie of locatie opgeslagen, wat de privacy verder waarborgt **Score: 5/5** (Dahan, 2024).
- **Transparantie over algoritmes:** Signal biedt volledige transparantie over hoe gegevens worden verwerkt en hoe hun algoritmes werken, dankzij de open-source aard van het platform. **Score: 5/5**.

Designproces

Inclusiviteit en gebruikersparticipatie

- **Toegankelijkheid voor mensen met beperkingen:** Hoewel Signal een sterk beveiligde app is, biedt het geen uitgebreide toegankelijkheidsopties zoals ondersteuning voor mensen met visuele of motorische beperkingen. Dit beperkt de toegankelijkheid voor sommige gebruikers **Score: 3/5** (Mann, 2024).
- **Gebruikersfeedback tijdens ontwerp:** Signal reageert goed op gebruikersfeedback en past regelmatig de functionaliteiten aan om de beveiliging en het gebruiksgemak te verbeteren **Score: 4/5** (Mocan, 2024).

Toegankelijkheid en gebruiksgemak

- **Gebruiksvriendelijkheid:** Signal heeft een eenvoudige en intuïtieve interface die gemakkelijk te begrijpen is voor gebruikers van alle niveaus **Score: 5/5** (Kaul, 2021).
- **Beschikbare handleidingen of hulppagina's:** Signal biedt uitgebreide ondersteuning via een FAQ en handleidingen op hun website, evenals directe ondersteuning via een helpdesk voor gebruikers met problemen **Score: 5/5** (Mann, 2024).

Ontwerpmethode

- **Privacy en toegankelijkheid in ontwerp:** Privacy staat centraal in het ontwerp van Signal, wat blijkt uit de standaard end-to-end encryptie en de minimale dataopslag. **Score: 5/5**.
- **Feedbackopties:** Signal biedt gebruikers eenvoudige manieren om feedback te geven, wat helpt om de app voortdurend te verbeteren **Score: 4/5** (Mocan, 2024).

Foundation

Mensenrechten en publieke waarden

- **Privacybescherming volgens de wet:** Signal voldoet aan de strengste privacywetten en biedt maximale bescherming voor gebruikersdata, omdat berichten end-to-end versleuteld zijn en er bijna geen data wordt verzameld **Score: 5/5** (Kaul, 2021).
- **Veilige opslag van gegevens:** Signal slaat geen berichten op hun servers op; alles blijft lokaal op het apparaat van de gebruiker, wat betekent dat de gegevens altijd veilig zijn **Score: 5/5** (Dahan, 2024).
- **Censuur en beperking van rechten:** Signal biedt volledige vrijheid van meningsuiting zonder beperkingen of censuur, en de communicatie is volledig versleuteld tegen inmenging door derden **Score: 5/5** (Dahan, 2024).

Governance en toezicht

- **Verantwoordelijkheid en transparantie:** Omdat Signal volledig open-source is, is het beheer van de app transparant, en gebruikers kunnen zelf controleren hoe hun gegevens worden verwerkt **Score: 5/5** (Dahan, 2024).
- **Onafhankelijke audits:** Signal ondergaat regelmatig onafhankelijke audits om de beveiliging en privacybescherming te verifiëren, wat helpt om vertrouwen te winnen bij de gebruikers **Score: 5/5** (Dahan, 2024).

Sociaal-economische impact

- **Toegankelijkheid voor iedereen:** Signal is volledig gratis te gebruiken en wordt gefinancierd door donaties, waardoor het toegankelijk is voor iedereen, ongeacht hun sociaaleconomische status **Score: 5/5** (Kaul, 2021).
- **Milieuvriendelijkheid:** Er is weinig informatie over de duurzaamheid van de infrastructuur van Signal, maar het gebruik van decentrale versleuteling vermindert mogelijk de belasting op hun servers **Score: 3/5** (Mocan, 2024).

Conclusie en samenvatting van de scores

Signal blinkt uit in privacy en veiligheid dankzij de volledige end-to-end encryptie, de open-source aard van de app, en de minimale dataverzameling. Het ontwerp is eenvoudig, gebruiksvriendelijk en volledig gericht op privacybescherming. Er zijn enkele kleine beperkingen op het gebied van toegankelijkheid en interoperabiliteit, maar over het algemeen is Signal een van de beste apps voor gebruikers die hun privacy willen beschermen.

Totaalscore:

- **Tech Stack:** 37/40
- **Designproces:** 22/30
- **Foundation:** 33/35

Signal scoort zeer hoog op alle lagen van de Public Stack en zet daarmee de standaard voor privacygerichte berichtendiensten.

Vergelijking van de Applicaties

Hier is een overzicht van de belangrijkste verschillen tussen Telegram en Signal, gebaseerd op de drie lagen van de Public Stack: Tech Stack, Designproces, en Foundation. Deze vergelijking laat zien welke applicatie beter scoort op publieke waarden en waarom.

Tech Stack

- Telegram gebruikt een eigen, gesloten encryptieprotocol, MTProto, dat minder gecontroleerd is door de open-source gemeenschap. Berichten zijn niet standaard end-to-end versleuteld, wat betekent dat Telegram de berichten op hun servers kan inzien, behalve in geheime chats.
- Signal maakt gebruik van volledig open-source end-to-end encryptie via het Signal Protocol voor alle berichten. Geen enkele derde partij, inclusief Signal zelf, kan de inhoud van berichten zien. Daarnaast verzamelt Signal minimale data, en de berichten worden nooit op hun servers opgeslagen.

Resultaat: **Signal scoort hoger** op het gebied van veiligheid en openheid, dankzij de standaard end-to-end encryptie en open-source karakter. Telegram heeft een minder transparante en veilige technische basis.

Designproces

- Telegram biedt beperkte toegankelijkheidsopties en houdt minder rekening met gebruikersfeedback, vooral op het gebied van privacy. Het ontwerp is vooral gericht op gebruiksgemak en snelheid, maar mist functies die de privacy van de gebruikers versterken.
- Signal heeft een minimalistisch, privacygericht ontwerp. Functies zoals verdwijnende berichten en veiligheidsnummers beschermen de privacy van de gebruiker op een eenvoudige maar effectieve manier. Signal is gebruiksvriendelijk en toegankelijk voor de meeste gebruikers.

Resultaat: **Signal scoort beter** door de sterke focus op privacy in het ontwerp. Telegram richt zich meer op gebruiksgemak, maar privacy krijgt minder prioriteit.

Foundation

- Telegram verzamelt meer gebruikersdata en slaat berichten op hun servers op, tenzij gebruikers geheime chats gebruiken. Het bedrijf is commercieel ingesteld, wat betekent dat er meer druk is om gegevens te verzamelen en winst te maken.
- Signal verzamelt vrijwel geen gebruikersgegevens, behalve een telefoonnummer. De app is non-profit en open-source, waardoor er geen commerciële belangen zijn die gebruikersdata in gevaar brengen. Signal biedt volledige transparantie en is vrij van advertenties.

Resultaat: Signal scoort aanzienlijk hoger in ethische verantwoordelijkheid en transparantie. Het open-source en non-profit karakter van Signal geeft het een sterke voorsprong op Telegram, dat minder transparant en commercieel gedreven is.

Belangrijkste verschillen en scores

- **Tech Stack**: Signal biedt volledige end-to-end encryptie en is open-source, terwijl Telegram een gesloten encryptieprotocol gebruikt en alleen geheime chats end-to-end encryptie bieden.
- **Designproces**: Signal is ontworpen met privacy als topprioriteit, met functies zoals verdwijnende berichten en gebruiksvriendelijkheid. Telegram richt zich meer op gebruiksgemak zonder dezelfde focus op privacy.
- **Foundation**: Signal is open-source, non-profit en volledig transparant over hoe het omgaat met data. Telegram verzamelt meer gegevens en heeft minder transparantie over de omgang met overheidsverzoeken en gebruikersdata.

Conclusie

Signal scoort op alle drie de lagen van de Public Stack beter dan Telegram. Signal biedt betere beveiliging door volledige end-to-end encryptie, een gebruiksvriendelijk en privacygericht ontwerp, en een transparante en ethisch verantwoorde basis dankzij het non-profit en open-source karakter. Telegram heeft veel gebruikers, maar scoort lager door het gebruik van een gesloten encryptieprotocol, minder sterke privacyopties, en een gebrek aan transparantie.

Verbetervoorstellen

Om Telegram meer in lijn te brengen met de publieke waarden zoals vastgelegd in de Public Stack, zijn er belangrijke verbeteringen nodig op het gebied van **techniek**, **ontwerp**, en **fundamentele waarden**. Hier volgen de belangrijkste aanbevelingen om de app te verbeteren:

1. Technische verbeteringen

- **Standaard end-to-end encryptie**: Telegram zou standaard end-to-end encryptie moeten invoeren voor alle communicatie, niet alleen voor geheime chats. Dit zou de privacy en beveiliging van gebruikers aanzienlijk verbeteren en voorkomen dat Telegram zelf of derden toegang krijgen tot gebruikersberichten. Dit zou de beveiliging naar het niveau van Signal tillen.
- **Open-source encryptieprotocol**: Telegram zou zijn **MTProto-encryptie** volledig open-source moeten maken. Hierdoor kunnen externe experts de code controleren en verbeteringen voorstellen. Dit zou het vertrouwen van de gebruikers vergroten en eventuele kwetsbaarheden sneller opsporen.
- **Data exporteren en interoperabiliteit**: Telegram zou zijn volledige MTProto-encryptie open-source moeten maken, zodat externe experts de code kunnen controleren en verbeteringen kunnen voorstellen. Dit zou het vertrouwen van de gebruikers vergroten en eventuele kwetsbaarheden sneller kunnen opsporen.

2. Design verbeteringen

- **Verbeterde toegankelijkheid**: Telegram zou de app toegankelijker moeten maken door opties toe te voegen voor schermlezers en spraakgestuurde bediening. Hierdoor kan de app beter gebruikt worden door mensen met beperkingen, zoals mensen met visuele of motorische beperkingen, wat de toegankelijkheid voor een groter publiek vergroot.
- **Actievere gebruikersbetrokkenheid**: Telegram moet actiever luisteren naar zijn gebruikers door hun feedback te integreren in het ontwerpproces. Dit kan de app effectiever maken en sneller laten inspelen op de behoeften van gebruikers.
- **Duidelijkere privacy-instellingen**: Telegram zou de privacy-instellingen veel transparanter en gebruiksvriendelijker moeten maken. Gebruikers moeten in één oogopslag kunnen zien welke gegevens worden verzameld en hoe ze deze veilig kunnen houden, wat hen uiteindelijk meer controle geeft over hun gegevens.

3. Fundamentele verbeteringen

- **Meer transparantie**: Telegram zou regelmatig transparantierapporten moeten publiceren waarin wordt vermeld hoe vaak overheden toegang vragen tot gebruikersdata en hoe hiermee wordt omgegaan. Dit zou het vertrouwen van gebruikers versterken dat hun gegevens goed beschermd blijven tegen ongewenste toegang.
- **Minimalisering van dataverzameling**: Telegram zou de hoeveelheid data die het verzamelt moeten beperken. Door alleen de noodzakelijke informatie, zoals telefoonnummers, te verzamelen, kan Telegram aantonen dat het serieus omgaat met de bescherming van gebruikersprivacy.

- **Verbeterde contentmoderatie**: Telegram zal moeten investeren in strengere vormen van moderatie om misbruik van het platform door criminele elementen en voor illegale activiteiten te voorkomen. Professionele moderatoren kunnen helpen om schadelijke inhoud in real-time te detecteren en te verwijderen, waardoor de veiligheid van het platform voor alle gebruikers wordt verbeterd.
- **Duurzaamheid**: Telegram zou stappen moeten ondernemen om het energieverbruik van zijn servers te minimaliseren. Dit kan worden bereikt door efficiëntere dataopslag en door limieten te stellen aan de duur dat berichten worden opgeslagen. Dit zou zowel bijdragen aan duurzaamheid als de privacy van gebruikers verbeteren.

Conclusie

Door deze verbeteringen door te voeren, zou Telegram op alle lagen van de Public Stack veel beter kunnen presteren. De app zou veiliger, transparanter en toegankelijker worden, en beter voldoen aan publieke waarden zoals privacy. Met deze verbeteringen kan Telegram een voorbeeld worden van hoe technologie op een ethische en verantwoorde manier kan worden gebruikt, iets wat Signal al grotendeels is.

Conclusie

In dit onderzoek heb ik twee van de meest populaire communicatie-apps vergeleken door hun prestaties op drie belangrijke aspecten te beoordelen: beveiliging, design en de foundation van de apps, met behulp van de Public Stack. Uit deze vergelijking heb ik kunnen concluderen dat Signal op alle niveaus van de Public Stack veel beter presteert dan Telegram, vooral op het gebied van privacybescherming, transparantie en ethische dataverwerking. Signal is daarom duidelijk te verkiezen boven Telegram, dat veel tekortkomingen vertoont, met name op het gebied van beveiliging, doordat het geen standaard end-to-end encryptie biedt en minder transparantie toont over hoe het omgaat met de data van gebruikers.

Wat heb ik geleerd?

Uit dit onderzoek blijkt hoe belangrijk het is dat technologie respect toont voor publieke waarden zoals privacy, toegankelijkheid en transparantie. Apps zoals Signal laten zien dat het mogelijk is om technologieën te ontwikkelen die de privacy van gebruikers respecteren en geen onnodige data verzamelen. Telegram daarentegen toont aan dat, zelfs bij populaire apps, privacybescherming niet voldoende wordt gegarandeerd, waardoor gebruikers kwetsbaar blijven. Dit onderzoek benadrukt hoe belangrijk het is dat technologiebedrijven deze publieke waarden respecteren, vooral wanneer ze beschikken over een grote gebruikersdatabase.

Aanbevelingen voor bredere toepassing van de Public Stack

Op basis van deze bevindingen raad ik aan dat techbedrijven de principes van de Public Stack integreren in hun ontwikkelingsproces. Dit betekent dat vanaf het begin rekening moet worden gehouden met privacy, toegankelijkheid en ethische dataverwerking. Bedrijven moeten technologie ontwikkelen die niet alleen veilig en transparant is, maar ook ethisch verantwoord. Door dit te doen, kunnen bedrijven niet alleen winst behalen, maar ook bijdragen aan het welzijn van gebruikers en de samenleving. Het is belangrijk dat meer bedrijven hun technologieën laten scannen aan de Public Stack. Zo kunnen we een technologische infrastructuur opbouwen die niet alleen commercieel gedreven is, maar ook de rechten en waarden van gebruikers respecteert en beschermt.

Literatuurlijst

Bruce Schneier. (2024, 9 september). *Telegram vs. WhatsApp: A Comprehensive Security Comparison for 2024*. 33Square. https://www.33rdsquare.com/telegram-vs-whatsapp/

Dahan, M., & Dahan, M. (2024, 9 maart). *How secure is Signal?* Comparitech. https://www.comparitech.com/blog/information-security/how-secure-is-signal/

Guneet Kaur. (2024, 30 augustus). *Telegram vs. WhatsApp — The encryption war*. CoinTelegraph. https://cointelegraph.com/learn/telegram-vs-whatsapp-encryption-war

Kaul, K. (2021, 26 juli). *Signal encrypted messaging review*. TechRadar. https://www.techradar.com/reviews/signal-encrypted-messaging

Mann, B. (2024, 27 april). *Signal Review 2024: Secure Messenger (Pros and Cons)*. RestorePrivacy. https://restoreprivacy.com/secure-encrypted-messaging-apps/signal/

Mocan, T., & Mocan, T. (2024, 2 september). *Signal vs. Telegram: Which Is Right for You in 2024?* SafetyDetectives. https://www.safetydetectives.com/blog/signal-vs-telegram/

Page, N. (2024, 25 september). The Myth of Telegram's Privacy: A closer look at its encryption shortcomings - Oak Park Journal. *Oak Park Journal*. https://oakparkjournal.com/technology/2024/the-myth-of-telegrams-privacy-a-closer-look-at-its-encryption-shortcomings/