Privacy Jam: *Secretum*

Introduction

In recent years, user privacy has been at the forefront of technological debates and concerns. The continued rise and popularization of technology has led many social media platforms to engage in what scholars describe as surveillance capitalism. The capitalization of user data results in an antagonistic model, where the interests of businesses and other organizational groups are structurally opposed to maintaining the privacy of its users.

This is even more relevant for protesters, a socially diverse group who are disproportionately targeted by law enforcement and other dataveillance agencies for their activities. This is significant as a report from the Center for Strategic and International Studies found that "mass protests increased annually by an average of 11.5 percent from 2009 to 2019 across all regions of the world" [1]. Protestors are also impacted by COVID-19 due to the introduction of health and safety protocols that prohibit regular meetings and informal organization. As physical and social distancing protocols are in place, organizations targeting climate change, youth gun violence prevention, Black Lives Matter (BLM) and others rely more on social media for organization and spreading awareness through digital activism [2].

In this environment we seek to create an alternative solution for data privacy. Our business model is designed to maximize security via conceptions of privacy that are built in from the conceptualization of the design. Incorporating a decentralized model with a defined server-client architecture allows Secretum to thoroughly allocate the central tenets of the operation toward these privacy and security ideals. Users will be able to engage socially with their peers while also having the opportunity to discover new groups and events based on locality or interest.

Background & Issues of Privacy

The problem with the encroachment on user privacy is outlined by Daniel Solove's [3] taxonomy of privacy. Defined are four main categories of privacy violations containing topics ranging from unwanted surveillance to personal intrusion. Solove creates this taxonomy to address the core issue relating to definition: privacy is difficult to define, regulate, and legislate. Privacy violations can incorporate a spectrum of issues that may not even always share a common denominator [3].

Shoshana Zuboff [4] presents surveillance capitalism as the way in which groups try to predict and modify user behaviours for profit and power. User data is continuously collected and sold to other parties, by these social media corporations, for economic profit. External parties can utilize this purchased information to analyze personal profiles, market a product to certain demographics, or even target the choice-making freedoms of their audience.

Issues of privacy and protection draw in wider debates surrounding what information can and should be collected, shared, and utilized, and how users may provide consent. The online sharing of personal data can lead to a whole range of real-life consequences, including threats to personal identity and safety. Privacy and the obtaining of information is not limited to large corporations. In the case of *Remsburg v. Docusearch, Inc.*, a client's information was sold to another individual, who utilized the personally identifiable data to locate, shoot, and kill the client [5]. The exploitation of personal data can be utilized for a whole range of unethical, illicit, or even criminal behaviours.

In other cases, such as the Cambridge Analytica controversy, it has been revealed that user data collected from social media may be utilized for electoral manipulation. Facebook's involvement in the scandal involves their role, or rather lack of, in protecting the data of its users. Personally identifiable data of over 87 million Facebook users were exposed when users falsely believed they were taking a personality test, when in fact, they were granting Cambridge Analytica access to their Facebook profile - and in turn, the data of all of their Facebook friends [6]. This data was then used to establish psychological profiles and predictions based on the social media activity of the users. Ultimately, the availability of the data provided the ability for firms, like Cambridge Analytica, to target individual consumers and voters, influencing their behaviour [6]. The degree to which Facebook was aware of this data breach is still contested, but this situation does reveal the extent to which many social media applications, such as Facebook, fail to protect its users. Personal information that is posted or shared no longer belongs to the individual. It is commodified to support these new emergent markets that seek to control and modify human behaviour. Online platforms have allowed traditional targeting techniques to be implemented in subtle ways, resulting in powerful techniques of influencing and tracking individual behaviours [8]. Data profiles generated from these sources of user information can contain anything and everything ranging from one's socioeconomic status to their psychological beliefs [8].

Issues of surveillance and privacy exist outside of the private sphere as well, with public sector groups also taking advantage. Historically, police and other government organizations have always used database style monitoring. In 2012, the Metropolitan Police in the United Kingdom were ordered to remove over 12 million photographs from their Police National Database. They were found to be using data from individuals who had never been charged with offenses in order to monitor public protest activities [9].

With the global adoption of social media, securing digital user privacy has never been more challenging. In the United States, law enforcement agencies have been documented for using digital surveillance to track protestors for years, enlisting telephone providers to relinquish names and phone numbers of those present at various events. A 2019 report from the New York Times found that cell phone developers and websites like Google can receive thousands of requests in a single month. These sources can be obligated to provide identifying information on hundreds of protestors if even a single crime is committed in the area [11].

Compounding this issue is the creation of Artificial Intelligence firms like Dataminr - a 2009 startup which has partnerships with many government agencies, including police and the CIA [12]. In 2016, Twitter was forced to divest in Dataminr after the American Civil Liberties Union (ACLU) found that it had been given direct access to every public tweet with full geospatial analysis functionality [13]. In an obtained email to law enforcement, Dataminr staff highlighted the use of this functionality in targeting and tracking activists and attendees at protests. Despite this public separation and updated Twitter privacy policies, Dataminr continues to provide social media surveillance through the collection and use of public tweets covering George Floyd, Black Lives Matter, and other examples of social activism [12]. This information is sold directly to police and other law enforcement groups and packaged to contain locations, activities, developments and instances of damage ranging from large protests to smaller planned events [14].

This form of surveillance capitalism is also widespread across mainstream social media platforms. In 2016, the ACLU found that Twitter, Facebook and Instagram provided social media monitoring data to Geofeedia, a developer who markets a consolidated product to law enforcement with the specific goal of reporting on activists and protests [15]. Instagram had provided access to all public Instagram user posts,

including location data tagged by users. Similarly, Facebook provided an API that generated a ranked feed of public posts focusing on desired events or places [15].

Once data is collected, data retention also becomes an issue to consider. One problem arising from data retention is the dissipation of social forgetfulness. Blanchette and Johnson [16] present this idea in relation to the social benefits of being able to start anew. The increasing amassment and hoarding of data create an inability for society to forget the past actions of users [16]. A petty crime committed as a child or a brash social media post made as a teenager may hold implications for a future job application decades down the road. Attendance at a protest may not be limited to present day complications but could hold great implications for the future. Anything that is shared online is seldom forgotten and users must be wary of data retention just as much as data collection.

This clearly demonstrates that there is a need for privacy solutions in the current context. These cases presented above unveil an industry rife with the abuse of user data and a penchant for violating their own privacy policies even after exposure. This is especially true for individuals who criticize law enforcement, government actions, or advocate for equity or action related to social initiatives. The goal of our decentralized platform is to deliver reliable digital and data security while providing information control and agency to this targeted group. Paired with a growing consumer mindset that is shifting towards privacy and market growth, a project exploring the creation of a privacy focused platform is relevant to the current climate and poised to disrupt an industry profiting off of surveillance capitalism.

Overview of Current Technologies

Our venture is not wholly unique in this ideal to an extent, as there are other social media offerings which focus on privacy. The most relevant to be reviewed are Mastodon, Signal, and Telegram. All three of these applications attempt to offer greater privacy marketed at the general audience.

Mastodon [17] is an open-source, self-hosted, decentralized networking service that functions a bit like Twitter and has around 2-3 million users. Detrimentally, it functions very similarly to Twitter, and draws into questions regarding unique and different functionalities. The basic premise of Mastodon is to allow anyone to create and operate their own social media platform. Due to its decentralization, the responsibility of privacy also falls on those who host a server. While this doesn't allow central entities like companies or institutions access to the data, it does enable privacy for radicalized groups [18]. However, because of this model, Mastodon does not have the ability to control and prevent its use by groups and users who may hold explicitly inappropriate views. In 2019 Gab, a social network prolific for hate speech, xenophobia and antisemitism moved to the platform. This resulted in a significant reputation hit for Mastodon as their platform has continued to allow far-right methodology in both content and communication [19].

This is one of the trade-offs of protecting and securing user privacy. Ensuring the privacy for one user ensures the privacy of all the others. At times, this may include groups who hold radicalized beliefs. No social media or communication network is perfect, but the ability to be able to provide users with the assurance that their data is kept confidential is at the forefront of this endeavor. Radicalized groups will always exist and may take advantage of secure technologies and networks, however the information protection of the average user is still a worthy cause. Some of these situations may be mitigated from strong content moderation but this is an issue that requires greater societal discussions and solutions. As our product is built on a decentralized model, general content moderation within groups and servers will be left to those applicable administrators and owners, however the Secretum team will maintain the right

to intervene in reported situations of legal copyright breach or or discovered illegal activity. The safety of the users are important but security and privacy still lie at the forefront of our goals.

Signal and Telegram are not platforms that function in the same wavelength as Mastodon. Telegram [20] launched in 2013 as a messaging app and is currently utilized by 400 million monthly users, designed to provide encrypted messaging and voice calls between individuals or groups. Telegram's published objective is to bring a reliable and secure chat messenger to the mass-market and they accomplish this via a cross platform application known for ease of setup, cloud storage and security via end-to-end encryption (e2e) [20]. However, in attempting to reach a broad audience, Telegram sacrifices this security by having e2e disabled by default to facilitate cross-system compatibility [20].

Signal's non-profit foundation system was created in 2018, dedicated to providing secure conversations, but they have operated as a secure messaging application under a few other names since a beta release in 2010 [21]. Signal also utilizes an end-to-end encryption protocol [22], but does not appear to succumb to the same weaknesses in their security as Telegram. They maintain that user's conversation and calls are completely secure and no trackers or marketing affiliates are involved in the system. Signal does what it claims to do well, which is provide users privacy for their messaging needs, but it is limited to this chat function.

Our Proposed Solution

Some users may not recognize some of the implications of privacy, contending that there is only such a worry if one has something illicit to hide [23]. However, as discussed, problems relating to surveillance and privacy exist in a diverse scope and hold implications for every single person. These sentiments are important to recognize as they prevail through much of popular discourse. It must be recognized that the 'I've got nothing to hide' argument is based on a narrow, individual conception of privacy and ignores many of the societal implications of information collection. It also operates under a presumption that the law adjudicates objectively and equally toward all citizens [23]. Many individuals appear to simply fail to recognize the importance of online privacy, especially when utilizing these social networks.

It is based on these popularized false assumptions and notions that we find necessary to create an application that allows for individuals and groups to convene and interact without being disenchanted by complex terms and conditions or vague privacy policies. While both Telegram and Signal are strong applications in their own right, both lack the integrative ability to search for users and groups to connect with, as well as a greater organizational platform for focused discussions within those group channels. Telegram and Signal offer increased messaging and calling privacy compared to many other popular applications on the market but are weak in the areas of generating new social connections and involvements with local and non-local groups and events.

Our biggest challenge in implementing this solution is to overcome the network effect and create organic growth. The network effect stipulates that when users subscribe to new technologies, the adoption rate corresponds to a sinusoidal function beginning at its minimum value at the point of introduction. User growth is relatively slow and stagnant until the user base reaches a critical threshold termed "the critical mass point" [24, p.5]. After this point the number of users quickly oscillates towards maximum saturation [24]. Achieving critical mass is often the most significant hurdle for new technologies.

We plan to achieve critical mass by targeting the same audience as many mainstream social media platforms, students. Facebook famously began as a student project only open to those with a Harvard email address before spreading to campuses all across North America within 10 months of existence [25]. While the same rate of growth cannot be anticipated, we explain why the student body is an ideal target audience in the next section, our Business Model.

Business Model

Target audience:

Protestors and activists are our target audience for this platform. As illustrated in our background, they are a high risk group for dataveillance and face significant complications related to privacy for which there are few options that compare to mainstream platforms like Facebook, Twitter and Instagram. Of those that exist, none are specifically tailored for organizing, facilitating and uniting these actors in their activities.

Furthermore, being in a student environment provides a distinct advantage for connection with this audience. A recent 2020 study by the Pew Research Center of over 9,000 US adults found that 41% of those who attended protests were younger than thirty [26]. Similarly, the average age of the US population enrolled in full-time undergraduate or graduate studies was 21.8 years old and part time students were 27.2 years of age as of 2018 [27]. In the Canadian context, the largest percentage of students enrolled in postsecondary institutions fell between the ages of 20 to 24 per a 2020 Statista Study [28]. This means that there is likely a large group of activists and protestors that are in post-secondary institutions, creating a perfect potential user base.

We plan to support local grassroots activism groups on campuses across Ontario as a mechanism for growth. Student associations often span cities across continents and by leveraging this communication highway we hope to rapidly grow our user base.

Business processes:

We leverage the ActivityPub protocol to create our privacy by design framework. This allows us to utilize an existing decentralized social networking protocol to create a platform that utilizes isolated servers to segregate data ownership from our operations.

Our product is designed to promote local growth in activism initiatives while providing a secure environment without any external data collection or capitalism. It differentiates itself from its competition by combining the messaging and call privacy of Signal and Telegram with the social interactivity of mainstream platforms like Facebook.

Like Signal and Telegram we plan to operate as an independent non-profit charity with all proceeds going towards running and improving the platform.

Business resources:

For our product, we plan to leverage the copyright infringement and digital millennium copyright act policies as Mastodon, another open source platform that utilizes ActivityPub. While we welcome and

encourage any collaboration as an open source software provider, we plan to take steps to protect ourselves from blatant infringement as we work with the community towards our common goal.

Value of Service:

For web-based platform services there are a number of pricing systems that are possible.

1. *Donation only Models:*

   Signal operates as a wholly free to use product. Their entire system is based on a donation system that utilizes one time or recurring payment structures [29].

   Telegram operates similarly, collecting donations via a Donate bot [30]. However, they also have their own funding provided by technology developer Pavel Durov and his brother.

2. *Subscription Based Models*

   Workplace from Facebook is another platform that provides collaboration and organization for different monthly subscription fees with various degrees of service provided [31]. This is a for profit model.

3. *Setup and Maintenance as needed Models*

   Within their Terms of Services, Mastodon allows for optional paid services, and upgrades via monthly or annual fees that are prepaid [32].

4. *Mixed Models*

   Although Mastodon uses the maintenance as needed model, they also accept donations and have some services that work as a recurring subscription [33].

We plan to examine pricing further following pilot implementation but will most likely employ a mixed model using donation and setup and maintenance as needed pricing indices.

Room for innovation:

The success and development of Mastodon across multiple devices is a testament to the level of engagement with their audience. Keeping our software open source allows us to collaborate with the community to further innovate and develop our product. Mastodon specifically has generated over 15 free and paid applications through community collaboration [34]. This demonstrates the viability of our open source approach as a mechanism for further development.

Legal Adherence

Privacy legislation is a highly localized phenomena, with each region or nation directing their own solutions based on their different political and social interpretations. In Canada, two main laws govern personal information and privacy: *The Privacy Act 1985* [35], and the *Personal Information Protection and Electronic Documents Act 2000* (PIPEDA) [36]. These two reigning documents serve as the general guidelines to regulating the collection, usage, and distribution of personal data, as well as providing

individuals with the legal authority of accessing their own personal data. The *Privacy Act 1985* [35] deals more with these rights of access and information dissemination in regard to government institutions. PIPEDA looks at a broader scope, dealing with protecting personal information that is accumulated or shared in commercial or workplace revenues [36].

While the stated purposes of both of these acts are to maintain personal privacy and provide greater autonomy to individuals regarding their own information, there exist numerous weaknesses, such as the ambiguity in what is deemed circumstantially appropriate personal information for an organization to collect [36]. Canadian legislature relating to privacy has also been critiqued for its inability to carry out enforcements of breaches [37]. PIPEDA outlines the rules that companies must follow relating to personal user information, but the Privacy Commissioner is limited in their enforcement abilities to actually hold these companies accountable [37]. The onus of one's own privacy is thrusted into the hands of consumers who must bear the responsibility of ensuring their social activities are not causing them due harm.

With that being said, social media platforms must still be wary of applicable legislation and the possibility of legal interventions. In 2016, Signal was the target of a subpoena by the Eastern District of Virginia [38]. The subpoena requested that Signal provide information regarding two users that were under investigation for a federal grand jury. Due to the privacy focused design of Signal and the minimal user data that is retained, the only information Signal produced was the date of a user's registration and their last connectivity to the platform [38]. Since Signal utilizes end-to-end encryption in combination with a minimal storage of user data, no records of messages, contacts, and group associations are able to be seen or exposed to the authorities [22].

Under PIPEDA regulations, personal information includes any personally identifiable data, including name, age, opinions; for the purposes of this report, our definition will remain the same. Business responsibilities under PIPEDA must follow the 10 fair information principles outlined in the act. The principles are accountability; identifying purpose; consent; limiting collection; limiting use, disclosure, and retention; accuracy; safeguards; openness; individual access; and challenging compliance [36]. As a non-profit endeavour, many of the corporate regulations would not apply, however abidance by PIPEDA and the fair information principles will still be honoured.

Accountability will be incorporated in this project by complying with all ten fair information principles. A transparent personal information and company practices policy will be developed and implemented to ensure continued responsibility. These public policies will also state the information that is being collected about the users, tying into the principles of consent and openness as well. It is the hope that we may strongly limit the collection of personal information in order to maintain user privacy in all stages. With the limited collection, the use and retention of personal information will be restricted to the bare operating requirements of the network system and user accessibility. Personal information will only be utilized and retained for necessary operational purposes, thus principle six of accuracy is not entirely relevant in this situation. User data and all of the information will be safeguarded by the strongest security protocols appropriate. Individuals may request access to their personal information if appropriate, although we foresee that very minimal amounts of information will be collected or retained. Any concerns from users or other organizations relating to the accountability of these 10 fair information principles and PIPEDA will be addressed in a timely manner.

Core Functionalities

Secretum utilizes four different tiers of organized communication accessible from a user's homepage. This screen provides a summary of a user's favourite communities, upcoming and past events, activity and is a nexus for accessing any of the four provided tiers

A. Servers

Upon logging into Secretum, users can create their own servers which can be organized by location, topic or interests. A preselection is presented based on individually selected interests which generate a customized experience.

B. Groups

Groups are associated under servers and provide channels for voice, text and video communication between members of that server. They also contain thread functionality for posts.

C. Events

Events can either be localized within servers or groups depending on their user-specified privacy settings. A public event organized in a location will show up in the events tabs for users who have that location's server flagged as an interest. Events can otherwise be restricted to users included in specific servers or groups within a unique server.

D. Messenger

All users have access to a messaging function which allows for group and individual chats between users and calls.

All four mechanisms utilize our search and filtering options for customized user experiences.

Technological Details

Architectural considerations

The presentation by Michael Schaus and Francis Szakacs [39] laid out four scenarios of data control and exchange. These four scenarios are separated by the two axes of transparency and decentralization. In short, there does not seem to be any argument for an opaque system that hides privacy considerations. Both "Data O Plomo" and "Big Data Brother" scenarios certainly have severe consequences for personal freedom and thus to the health of our society [16]. The issue of decentralization seems to be a bit more complicated.

Centralized vs decentralized

Decentralization has been pushed as a solution to oppose the central powers of data conglomerates like Facebook or Google. In doing so, it has not been always clear what decentralization means [40]. Vitalik Buterin, the co-founder of Ethereum, places decentralization on three separate axes: architectural, political and logical [40]. Architectural decentralization refers to the number of physical computers that

make up a system and how many of them can fail. Political decentralization refers to how many individuals or organizations ultimately control these computers. Finally, logical decentralization refers to interface and whether it is experienced as a single monolithic object or as an amorphous swarm [40].

Decisions on these axes do not only address the issue of privacy but also power and user experience. All of them must be considered. For example, while a large number of decentralized computers can make it difficult to attack the system and control it (as there is no single point of failure), there are financial and timely costs associated with the set-up and maintenance of these computers. Furthermore, it can be comfortable to transfer power to organizations if it means a reduced workload and increased convenience. Finally, a decentralized user interface can break the flow of good user experience which ultimately has consequences on the uptake of the system. The analysis of the ActivityPub protocol can help finding a healthy placement on any of these three axes of decentralization.

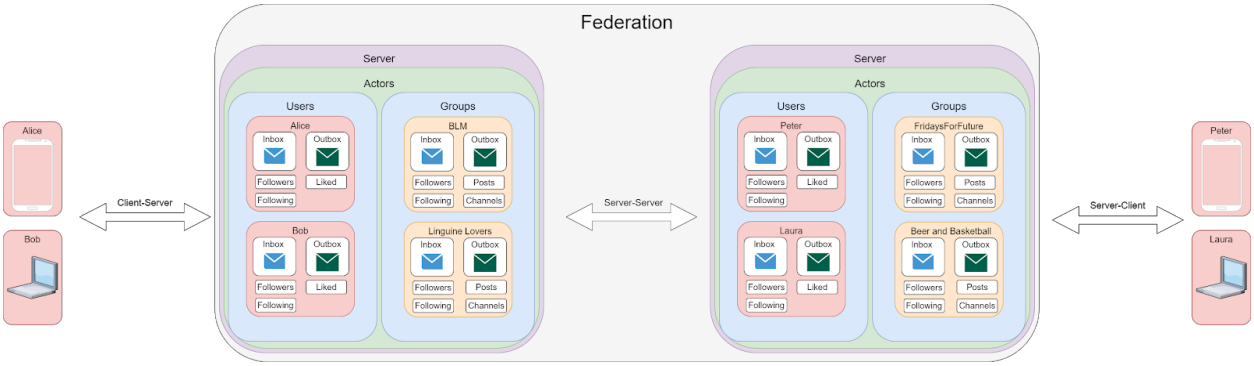
ActivityPub

The ActivityPub protocol is a decentralized social networking protocol [41] that is already in use in platforms like Mastodon. It is built on a server-client architecture and allows the communication of users with and between servers. Insofar, the ActivityPub protocol directly enables architectural and political decentralization through the independence of single servers that can be set up by everyone. Here, architectural decentralization leads to political decentralization of power if servers can be run without impact from anyone, including the creators of social network applications. Furthermore, interfaces can be created in a cohesive way that allows seamless interaction with users across servers. Because of those benefits and the fact that ActivityPub is already used, we decided to use it for our network. Therefore, decentralization enabled through ActivityPub, which transfers power and data ownership from the few to the many, constitutes to be one of our core pillars of privacy by design.

Peer to peer (P2P) vs server-client

ActivityPub defines a server-client architecture. This architecture comes with advantages and disadvantages compared to P2P networks, in which users also offer a part of their compute resources as a small computational node to the network. P2P, for example, is easy to set up and relatively cheap since servers do not need to be set up or maintained. These advantages would solve the problem that we try to solve in our business model proposal. However, due to disadvantages we decided against P2P. The main disadvantage we see is the implicit sharing of compute resources that users either find annoying or intimidating. Furthermore, the collaboration of multiple users in a group is difficult to organize in a P2P network. Finally, a P2P network introduces a threat to security as viruses and malware can be introduced to private computers.

Architectural overview



An overview of the architecture is given in Figure 1. It shows the users Alice, Bob, Peter, and Laura communicating with their phones, laptops and other devices on our network. This network can be described as a Federation of servers for which the ActivityPub protocol defines the communication between servers and between servers and clients (i.e., users). Each server holds Actors that are key objects in the ActivityPub protocol. These actors are either individual users or groups that all have inboxes and outboxes that are key components of data management in the federation. While the ActivityPub is flexible enough to define both users and groups as Actors, the definitions of these classes can be appended with additional data fields that hold posts and channels for groups or a list of liked objects for users. In the following description, we lay out some common operations to provide a better understanding of our network:

1. Alice want to view the posts on their timeline:
    a. Alice sends a GET-request to their server
    b. The server sends back ActivityStream objects (basically a JSON file) that are gathered in Alice's inbox and that can be viewed on Alice's phone
2. Alice want to send a message to Laura:
    a. Alice sends a POST request to their outbox on their server (i.e., client-server)
    b. Alice's server checks the message, finds that the message is addressed to Laura, and sends the message to Laura's server (i.e., server-server)
    c. Laura's receives the message and places it in Laura's inbox
    d. Laura sends a GET-request to their server to receive Alice's message
3. Bob creates a post in Linguine Lovers:
    a. Bob sends a POST request to their outbox on their server (i.e., client-server)
    b. Bob's server checks the message, finds that the message is addressed to Linguine Lovers, and places the post into the inbox of Linguine Lovers
    c. Bob's server finds the list of followers of Linguine Lovers (i.e., Alice and Peter) and sends out Bob's post to the inboxes to all followers
    d. Alice and Peter send a GET-request to their server to receive Bob's post from their inboxes

Private groups and messages

ActivityPub is optimized for public social network activities like liking, sharing and commenting on media content (e.g., text, images, etc.). It does not natively support private direct messages between users [42]. Furthermore, the creation of private groups is difficult to realize. ActivityPub allows to send non-public

content to specific lists of users' inboxes or into shared inboxes which effectively leads data to trickle throw the decentralized network. For private groups, however, it might be useful to keep the data in one place that can be accessed with proper authentication directly from all users of that group. Besides these issues the protocol also lacks the ability for users to migrate between servers and to have nomadic identities on multiple servers simultaneously that allow users to still have access to the network if their original server goes down [43]. To mitigate this issue our network could partly rely on the Zot protocol [44]. Nonetheless, ActivityPub is widely adopted which makes it beneficial (e.g., cross-platform communication to users of Mastadon, PeerTube, etc.) to adopt for us, too.

End-to-end encryption vs server-side encryption

ActivityPub comes with server-side encryption meaning that communications from and to the server are encrypted while the data itself is visible to the server and its administrator. This access to information provides a potential point of failure where security is preached by administrators that spy on its users. To overcome this issue, end-to-end encryption has been proposed to be added to ActivityPub [45]. While this would ensure that administrators don't have access to data it comes with disadvantages, too: server-side effects of messages are hard to realize, the maintenance of keys is a difficult UX problem, and key recovery provides a challenge [46]. As a remedy, developers of ActivityPub have argued to "just run your own server" [45]. However, we think that this provides a severe barrier to mainstream uptake. To remedy this issue, a solution can be found on an application level where certain functionality (e.g., secret chats akin to Telegram) can be based on end-to-end encryption while the rest of the network (e.g., subscribing, sharing, liking) can be based on the ActivityPub protocol. Nonetheless, we consider privacy literacy of users on who is running servers a key challenge.

References

[1] https://www.csis.org/analysis/age-mass-protests-understanding-escalating-global-trend
[2] https://www.theverge.com/2020/3/13/21178376/activists-phones-online-coronavirus-protests
[3] https://www.law.upenn.edu/journals/lawreview/articles/volume154/issue3/Solove154U.Pa.L.Rev.477(2006).pdf
[4] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2594754
[5] https://www.lexisnexis.com/community/casebrief/p/casebrief-remsburg-v-docusearch-inc
[6] https://ieeexplore.ieee.org/stamp/stamp.jsp?tp=&arnumber=8436400
[7] http://www.berghel.net/col-edit/out-of-band/may-18/oob_5-18.pdf
[8] https://policyreview.info/articles/analysis/voter-preferences-voter-manipulation-voter-analytics-policy-options-less
[9] http://www.bailii.org/ew/cases/EWHC/Admin/2012/1681.html
[10] https://www.documentcloud.org/documents/6935331-UCB-Search-Warrant.html
[11] https://www.nytimes.com/interactive/2019/04/13/us/google-location-tracking-police.html
[12] https://theintercept.com/2020/07/09/twitter-dataminr-police-spy-surveillance-black-lives-matter-protests/
[13] https://www.aclu.org/blog/privacy-technology/internet-privacy/twitter-cuts-fusion-spy-centers-access-social-media
[14] http://www.aclunc.org/docs/20151130_dataminr_email_to_lapd.pdf
[15] https://www.aclunc.org/blog/facebook-instagram-and-twitter-provided-data-access-surveillance-product-marketed-target
[16] https://www.tandfonline.com/doi/abs/10.1080/01972240252818216
[17] https://joinmastodon.org/
[18] https://www.theverge.com/2019/7/12/20691957/mastodon-decentralized-social-network-gab-migration-fediverse-app-blocking
[19] https://blog.joinmastodon.org/2019/07/statement-on-gabs-fork-of-mastodon/
[20] https://telegram.org/faq#q-what-is-telegram-what-do-i-do-here
[21] https://increment.com/security/story-of-signal/
[22] https://signal.org
[23] https://papers.ssrn.com/sol3/papers.cfm?abstract_id=998565
[24]https://www.researchgate.net/publication/220437008_Exploring_the_role_of_network_effects_in_IT_implementation_The_case_of_knowledge_repositories
[25] https://www.brandwatch.com/blog/history-of-facebook/
[26] https://www.pewresearch.org/fact-tank/2020/06/24/recent-protest-attendees-are-more-racially-and-ethnically-diverse-younger-than-americans-overall/
[27] https://educationdata.org/college-enrollment-statistics
[28] https://www.statista.com/statistics/450253/enrollment-of-postsecondary-students-in-canada-by-age-and-gender/
[29] https://signal.org/donate/
[30] https://t.me/telegramdonate
[31] https://www.workplace.com/pricing
[32] https://discourse.joinmastodon.org/tos
[33] https://joinmastodon.org/sponsors
[34] https://joinmastodon.org/apps
[35] https://laws-lois.justice.gc.ca/eng/acts/P-21/FullText.html#h-397260
[36] https://laws-lois.justice.gc.ca/ENG/ACTS/P-8.6/page-1.html

[37] https://www.theglobeandmail.com/business/commentary/article-thank-facebook-for-reminding-us-canadas-privacy-protection-is-utterly/
[38] https://signal.org/bigbrother/eastern-virginia-grand-jury/
[39] https://www.youtube.com/watch?v=UXXM95ce8-A
[40] https://medium.com/@VitalikButerin/the-meaning-of-decentralization-a0c92b76a274
[41] https://www.w3.org/TR/activitypub
[42] https://github.com/w3c/activitypub/issues/196
[43] https://wiki.freedombone.net/view/welcome-visitors/view/a-peoples-history-of-the-fediverse/view/protocol-wars/view/the-ideal-protocol
[44] https://zotlabs.org/help/en/developer/zot_protocol
[45] https://github.com/w3c/activitypub/issues/225#issuecomment-304938193
[46] https://github.com/WebOfTrustInfo/rwot5-boston/blob/master/draft-documents/activitypub-decentralized-distributed/activitypub-decentralized-distributed.md#fn.8