

Choosing Your Friends: Shaping Ethical Use of Anonymity Networks

Daniel Huguenroth^[0000–0003–3413–1722],
Ceren Kocaoğullar^[0000–0002–4260–2953], and
Alastair R. Beresford^[0000–0003–0818–6535]

University of Cambridge, United Kingdom

Abstract. Anonymity networks protect the metadata of communication between participants. This is an important privacy guarantee for whistleblowers, activists, journalists and others who rely on anonymity networks. However, these same guarantees can also help criminals and disruptive users evade the consequences of their actions. Existing literature and research has little to say on what designers and operators of such networks can do to maximize beneficial uses while minimizing harm. We build on lessons learned from the widespread deployment of another strong privacy technology, end-to-end encrypted messaging applications, as well as on existing examples from anonymity networks, to formulate a set of design methods which anonymity networks can use to discourage harmful use. We find better solutions exist when networks are specialized to particular application domains since such networks are then able to provide a better trade-off between benefits and harms. One drawback of such specialization is that it may lead to smaller numbers of users and therefore an increased risk of insufficient anonymity.

Keywords: anonymity · ethics · socio-technical · dual-use.

1 Introduction

End-to-end encryption (E2EE) has become a typical feature in messaging apps for providing strong message confidentiality. Mobile apps like WhatsApp, iMessage, and Signal brought this leap in privacy to billions around the world — and with it, concerns for its potential for abuse. At the same time, metadata, such as who talks to whom and when, remain readily available for passive network observers and platform operators.

Anonymity networks are overlay networks that hide such metadata. This active research area traces back to the seminal work by Chaum [3] and has led to several distinct design patterns including onion routing, mix networks, and DC-Nets. Anonymity networks do not only exist on paper — examples such as Tor [8], I2P [21], and Nym [7] are deployed on many nodes across continents. Over the years, such networks have improved steadily and now achieve high-bandwidth, low-latency communication that can resist powerful adversaries.

Similarly to E2EE, anonymity networks are dual-use technologies. On one hand, they are critical tools for good: they protect sources that reach out to journalists [6] to blow the whistle on wrongdoing inside powerful organizations; and they protect the identities of activists, civil servants, and non-governmental organizations working in precarious conditions. On the other hand, anonymity networks are also susceptible to exploitation by malicious actors. They can enable criminal organizations to evade scrutiny from law enforcement or at least achieve plausible deniability; they offer the infrastructure for anonymous online drugs and arms market places [4]; and they allow individuals to spread misinformation and harassing messages without direct accountability.

Understandably, anonymity researchers tend to highlight the many positive uses and few papers reflect on the potential for misuse. The Tor project’s abuse FAQ addresses the question “Doesn’t Tor enable criminals to do bad things?” [20] arguing that criminals can already carry out illegal activities using other methods, such as stealing cell phones or cracking into computers (see Appendix A for the full quote). However, we believe that this argument fails to consider the varying levels of resources, professionalism, and expertise available to different types of malicious actors. For an opportunistic criminal a readily available anonymity network might reduce hesitation and provide an easy and effective means of evading detection.

It is important for our community to recognize the potential for misuse and address the ethical challenges associated with anonymity networks to ensure that their benefits are not outweighed by their risks. In this paper, we argue that anonymity network designs should more explicitly consider and encourage good usage while simultaneously disincentivizing improper exploitation. While there is no silver bullet, we highlight several design choices that can limit the potential for abuse.

The real world is often not clear-cut into good and bad, and there are many gray areas where context matters. Therefore, we frame our decisions in context of maintaining control over who uses the technology and for what purposes. For this paper we group our design decisions into four categories: Anonymity restrictions (§2), technical limitations (§3), communication and content topology (§4), and safeguards (§5).

2 Anonymity restrictions

While the term “anonymity” is often used broadly, it is an inherently relative property describing the relation between the user who tries to stay anonymous and a counter party who is interested in identifying them. Hence, it is only meaningful if we know the group towards whom users and their actions are meant to be anonymous. Unfortunately, many designs often lack precise and deliberate discussion of these relationships. In this section we present three design choices that intentionally limit anonymity guarantees towards certain parties in order to discourage abuse.

One-sided anonymity. Reducing the peer-to-peer characteristics of an anonymity network can be an effective way to limit unintended activities. One way to achieve this is to restrict regular users to selecting communication partners only from a curated list, which can be maintained by the network operators. This prevents unregulated exchanges between arbitrary users and thwarts ambitions to organize criminal activity or run online market places.

An example for such a design choice is found in the CoverDrop [1] anonymity network. CoverDrop allows users of a news app to reach out securely and anonymously to journalists of the news organization that runs the network. However, the journalists are not anonymous towards the users who can verify who they are talking with. As the users of the app are limited to communication with the journalists, they are unable to communicate with one another. A single node controlled by the news organization enforces the routing. Ultimately, the designers of the system trust the journalists to act responsibly and ethically with the information shared through the system and that they are able run the infrastructure properly.

Knowing your users. Not all anonymity networks require the entire global population as its potential anonymity set. Direct deployment for trusted governmental organizations and industrial companies can provide strong anonymity for a selected set of users while keeping it out of reach of others.

The industry of encrypted smartphones provides well-known examples where this principle was applied for the opposite effect. The EncroChat smartphone was directly distributed as a turnkey solution to criminal organizations [9]. A similar encrypted communication platform, Phantom Secure, exposed its founder and associates to criminal charges under Racketeer Influenced and Corrupt Organizations Act (RICO) in the US [10]. While targeted deployment of anonymity networks can be exploited for nefarious purposes, as evidenced by the cases of EncroChat and Phantom Secure, the same approach can also be effective for securing communication among specific groups, such as government agencies or corporations.

Non-anonymous access. Most anonymity networks that are practically deployed allow access to everyone without identity verification. For instance, access to Tor [8] is offered for free and the Nym network [7] allows payment with anonymous tokens. This is in line with common expectations of an anonymous system, but it also limits the operator’s ability to exclude malicious users or comply with legal regulations, such as economic sanctions.

However, an anonymity network does not necessarily require anonymous access to provide anonymity. For example, an operator could require identification of its users and run a subscription system that then gives the user short-lived access tokens. Such an approach would not affect the anonymity provided within the network, while allowing the operator to demonstrate due diligence. If a user is later revealed to be undesirable, for instance they are sentenced as a member of a criminal organization, their access can be revoked.

3 Technical limitations

Many designs consider technical limitations as a negative property that is often only characterized during the evaluation of the final system. However, we can deliberately introduce technical limitations to limit nefarious use of an anonymity network.

Bandwidth. A system may not be well-suited for certain activities or content because of its bandwidth requirements and achievable application-level goodput. For example, many mix network designs hide communication patterns by setting sending rates independently of communication rate. When no messages are available, so-called cover messages are sent instead. One such design is Loopix [17]. Given a pre-determined sending rate and the fact that all messages are the same size, the throughput of any underlying communication is severely limited. This design choice typically renders such networks only suitable for exchanging short text messages. Consequently, such networks are not an appropriate medium for distributing exploitative image or video material anonymously.

Latency. Similarly, network latency can be an inhibitor of certain applications. For instance, many DC-net designs require synchronized rounds for transmitting information between their clients. This fundamentally rules out low-latency applications, such as Voice-over-IP or real-time remote control of drones and robots.

Free and open distribution. Both practically deployed anonymity networks and academic research prototypes are typically shared as open-source. Without existing trust relationships between the operator and the user, this approach is seen as necessary to foster trust in the software. However, unrestricted availability of the source code also can expose the network to potential misuse by unauthorised groups. For instance, a network designed for hidden communication within NGOs could be deployed by criminal organizations to run their illicit operations. Moreover, the accessibility of the source code enables these groups to modify the software to suit their specific requirements. For instance, if a network was designed to permit only text messages, the code could be altered to create a version that permits image sharing.

4 Communication and content topology

Content and information discovery mechanisms can have a significant impact on how information spreads within a communication system and what social dynamics develop. Therefore, when designing any such system, be it anonymous or not, it is crucial to carefully consider these mechanisms.

Shared index. A common mechanism for discovering content is to have a shared index, for example a distributed hash table, that can be searched by users. In particular, such an index provides new users with value from the get-go, as they can simply query it for the content they are interested in without having to perform any other interactions. However, a searchable index might make an anonymity network more suitable for file-sharing and online marketplaces, which may not be desirable in a platform where pirating or trade of illicit goods are concerns.

Subscriber-based systems. Other networks, in particular social media platforms, adopt a graph based topology where users subscribe to topics and people that they are interested in. However, these mechanics have to be employed carefully as they otherwise can cause negative effects. For example, the algorithmic feeds of Facebook, Instagram, and more recently TikTok have attracted concern, as they are suspected to amplify controversial content and misinformation [19, 12, 16].

One-to-one contact establishment. As an alternative to these discovery mechanisms, content might be directly shared between users. This can be implemented by following individual accounts, like on Twitter, or by allowing users to find and directly contact users through information in their contact address books, as in WhatsApp. Such network structures make sharing and finding information inherently less scalable. However, they are not necessarily immune to quick spread of misinformation, as has been observed in E2EE messaging applications that employ one-to-one contact establishment. WhatsApp addressed this challenge by limiting the number of times that a message can be forwarded [13].

5 Safeguards

Our final set of design choices comprises policy decisions that promote use-case alignment with the operator’s interests and can safeguard external entities from negative effects.

Alignment of trust. Anonymity network users rely on network operators to safeguard against a critical number of malicious nodes that could compromise the network’s integrity. This trust is often established by dividing control of network nodes among multiple independent operators. If a sufficient portion of the nodes are run by operators with competing incentives, it is unlikely that they would collude to compromise users’ anonymity — as it is the case with Tor [8].

Alternatively, operator responsibility could be delegated to organizations that share a common cause. For example, a consortium of news organizations can be trusted to defend the anonymity of whistleblowers. However, it is unlikely that they would provide protection for criminal activities on an anonymity network that they control. This setup renders the network non-trustworthy for illicit actors and hence the misalignment of trust acts as a deterrent.

Interaction with external resources. Anonymity networks might interact with external resources, where they serve as a layer of obfuscation between the user and, for instance, regular websites. VPN services and projects like AN.ON/JAP [14] allow users to browse the Internet anonymously, while Tor [8] provides access to both internal resources (Hidden Services) and the Internet through exit nodes. However, while accessing existing content and websites can make an anonymity network more appealing to new users, these resources may not be equipped to handle anonymous requests. As a result, allowing anonymous access to these services can make them vulnerable to vandalism and abuse, which in return harms regular users and threatens the reputation of the anonymity network.

Anonymity networks can reduce this risk for external services. For example, Tor publishes a complete list of its exit nodes, which allows websites to implement extra protection measures such as CAPTCHAs or blocking access entirely from the Tor network. Anonymity networks can also limit connections to external resources. For instance, Tor exit node operators can employ so-called exit policies to restrict certain types of traffic. The default exit policy blocks port 25, which prevents sending spam messages using SMTP via the Tor network.

6 Related work

The 1999 ACM Code of Ethics [11] asks software practitioners to “identify, define, and address ethical [...] issues related to work projects”. However, we have found little existing work specifically addressing the ethical considerations of anonymity network research and how it is formed by technological choices. In this section, we highlight related work that tackles similar ethical questions about anonymity and anonymity networks.

In his article “The Moral Character of Cryptographic Work” [18] Rogaway argues that cryptography influences power relations and is inherently political. Specifically, he advocates for the development of effective methods to combat mass surveillance, a cause that we endorse as well, and in which anonymity networks play a pivotal role. Rogaway states that scientists who are socially engaged are expected to have a clear and well-defined ethical perspective on how their work in their respective fields should affect society. We hope to make a modest contribution with this paper.

Data on how anonymity networks are used is inherently difficult to come by due to privacy properties they offer. Jardin et al. use the relative volume of connections to Hidden Services versus regular websites as a probabilistic proxy metric [15], finding that Hidden Services are disproportionately used for illicit use, while regular website use is more moderate due to discoverable administrators and hosting providers. One interesting observation is that the ratio in “free countries” is skewed towards the former, whereas the latter is more popular in “non-free countries”.

The discussion of real-name policies on social media platforms has received significant attention recently. While it is (only) considering pseudonyms, it is in-

teresting as the discourse typically assumes that individuals who use pseudonyms are effectively anonymous. The work by Bodle provides a summary of the ethical considerations, arguing that anonymity is “indispensable as an enabler of other inalienable rights” [2, p.22] and can encourage “honest self-disclosure” [2, p.26]. However, Bodle concedes that the issue evades a utilitarian approach because consequences might not be foreseeable, and instead favors an ethical pluralist approach.

Social dynamics similar to our considerations of one-sided anonymity and alignment of trust have been previously considered in the context of peer-to-peer networks and their censorship resistance. The work by Danezis and Anderson compares the economic differences between a “random model” where content is indiscriminately stored on random nodes and a “discretionary model” where content is only shared by those who also consume it [5]. Similar analysis of social dynamics in the context of anonymity networks and embedded communities might be interesting to better understand trade-offs.

7 Conclusion

This paper has highlighted several design choices that can make anonymity networks more specialized and suitable for specific scenarios, which in turn can limit their potential for abuse and misuse. In its simplest form, networks can restrict access to only a vetted group of people, or limit the communication so that one side is trusted. Similarly, a network that can only transport small text messages will not appeal to those trying to share exploitative videos. Where a network interacts with external resources, connection filters can reduce the potential for abuse and preserve the network’s reputation.

We can also learn from the existing experiences and discussions on encrypted messaging platforms. Inconspicuous features like forwarding messages can fuel the spread of misinformation where the original source becomes oblivious to the recipients. A counter-argument would be to rely on the user to critically examine information and challenge it. However, experience with E2EE messaging apps has shown that reliance on the user does not hold up when technology gains mainstream popularity.

We believe that anonymity networks are predominately a force for good and that they help to protect vulnerable groups and people. However, even if illicit use is rare, it can risk the reputation of the entire network. It seems inevitable that anonymity networks become a target in public discourse as they grow more capable, popular and successful. Our ability to defend the benefits of anonymity networks will be strengthened by proactively addressing and incorporating ethical considerations into our research and development processes.

While this paper focuses on the use of anonymity technology, there are other pressing ethical challenges. For instance, there are ecological implications of cover messages for hiding communication patterns, which lead to more data transmission and hence energy consumption. Also, the question of access to technology is

important: how do such networks contribute to inequality if they are primarily accessible to a small, educated elite?

In our accompanying talk, we hope to inspire discussion on the research in this field. In particular, we are hoping to see more anonymity networks escape the all-purpose setting and concentrate on particular use-cases. Such an approach allows app-specific methods of limiting potential abuse while simultaneously encouraging new ideas and therefore innovation. One drawback of such specialization is that it may lead to smaller numbers of users and therefore an increased risk of insufficient anonymity. Balancing these benefits and drawbacks will be a defining feature of such future systems.

Acknowledgments

The authors would like to thank Laura Bechthold and Jenny Blessing for interesting discussions and valuable feedback before the workshop. In addition, the authors would like to thank all workshop participants whose questions and input helped shape this revised paper version. Daniel Hugenothe is supported by Nokia Bell Labs and the Cambridge Trust. Ceren Kocaogullar is supported by King’s College Cambridge and the Cambridge Trust.

References

1. Ahmed-Rengers, M., Vasile, D.A., Hugenothe, D., Beresford, A.R., Anderson, R.: Coverdrop: Blowing the whistle through a news app. *Proceedings on Privacy Enhancing Technologies* **2022**(2), 47–67 (2022)
2. Bodle, R.: The ethics of online anonymity or Zuckerberg vs. Moot. *ACM SIGCAS Computers and Society* **43**(1), 22–35 (2013)
3. Chaum, D.L.: Untraceable electronic mail, return addresses, and digital pseudonyms. *Communications of the ACM* **24**(2), 84–90 (1981)
4. Christin, N.: Traveling the Silk Road: A measurement analysis of a large anonymous online marketplace. In: *Proceedings of the 22nd international conference on World Wide Web*. pp. 213–224 (2013)
5. Danezis, G., Anderson, R.: The economics of resisting censorship. *IEEE Security & Privacy* **3**(1), 45–50 (2005)
6. Di Salvo, P.: Securing whistleblowing in the digital age: SecureDrop and the changing journalistic practices for source protection. *Digital Journalism* **9**(4), 443–460 (2021)
7. Diaz, C., Halpin, H., Kiayias, A.: The Nym Network. Whitepaper (2021)
8. Dingledine, R., Mathewson, N., Syverson, P.: Tor: The second-generation onion router. Tech. rep., Naval Research Lab Washington DC (2004)
9. Europol, Eurojust: Dismantling of an encrypted network sends shockwaves through organised crime groups across Europe (2020), <https://www.europol.europa.eu/media-press/newsroom/news/dismantling-of-encrypted-network-sends-shockwaves-through-organised-crime-groups-across-europe>, accessed January 2023
10. Federal Bureau of Investigation: International criminal communication service dismantled (2018), <https://www.fbi.gov/news/stories/phantom-secure-takedown-031618>, accessed January 2023

11. Gotterbarn, D., Miller, K., Rogerson, S.: Software engineering code of ethics is approved. *Communications of the ACM* **42**(10), 102–107 (1999)
12. Hern, A.: Instagram led users to Covid misinformation amid pandemic – report. *The Guardian* (2021), <https://www.theguardian.com/technology/2021/mar/09/instagram-led-users-to-covid-misinformation-amid-pandemic-report>, accessed January 2023
13. Hern, A., Safi, M.: WhatsApp puts limit on message forwarding to fight fake news. *The Guardian* (2019), <https://www.theguardian.com/technology/2019/jan/21/whatsapp-limits-message-forwarding-fight-fake-news>, accessed January 2023
14. JAP Team: Project: AN.ON - anonymity.online (2011), https://anon.inf.tu-dresden.de/index_en.html, accessed January 2023
15. Jardine, E., Lindner, A.M., Owenson, G.: The potential harms of the tor anonymity network cluster disproportionately in free countries. *Proceedings of the National Academy of Sciences* **117**(50), 31716–31721 (2020)
16. Paul, K.: We risk another crisis: TikTok in danger of being major vector of election misinformation. *The Guardian* (2022), <https://www.theguardian.com/technology/2022/oct/24/tiktok-election-misinformation-voting-politics>, accessed January 2023
17. Piotrowska, A.M., Hayes, J., Elahi, T., Meiser, S., Danezis, G.: The Loopix anonymity system. In: 26th USENIX Security Symposium (USENIX Security 17). pp. 1199–1216 (2017)
18. Rogaway, P.: The moral character of cryptographic work. *Cryptology ePrint Archive* (2015)
19. The Economist: How social-media platforms dispense justice. *The Economist* (2018), <https://web.archive.org/web/20190516115755/https://www.economist.com/business/2018/09/06/how-social-media-platforms-dispense-justice>, accessed January 2023
20. Tor Project: Abuse FAQ - Doesn't Tor enable criminals to do bad things? (2023), <https://support.torproject.org/abuse/what-about-criminals/>, accessed February 2023
21. Zantout, B., Haraty, R., et al.: I2P data communication system. In: *Proceedings of ICN*. pp. 401–409. Citeseer (2011)

A The Tor FAQ entry

The following is a full quote from the Abuse FAQ of the Tor project [20] retrieved on 14th February 2023.

Doesn't Tor enable criminals to do bad things?

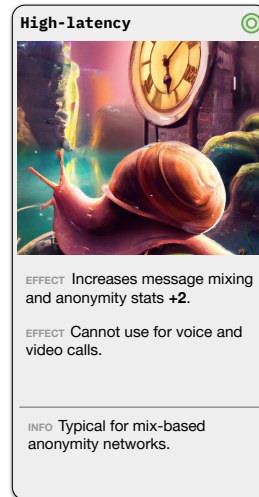
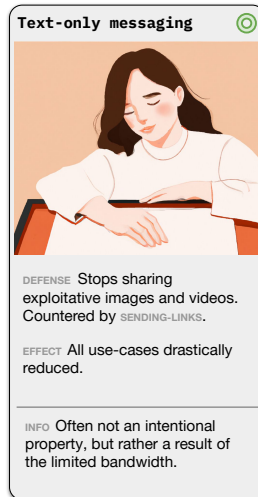
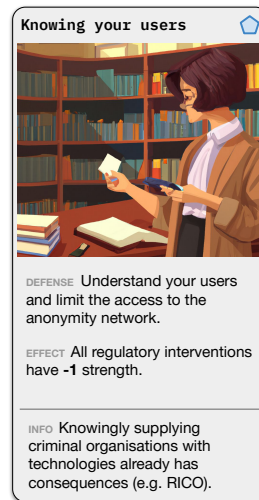
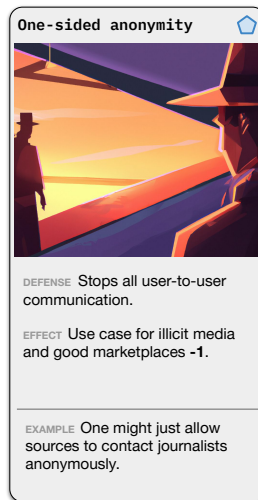
Criminals can already do bad things. Since they're willing to break laws, they already have lots of options available that provide better privacy than Tor provides. They can steal cell phones, use them, and throw them in a ditch; they can crack into computers in Korea or Brazil and use them to launch abusive activities; they can use spyware, viruses, and other techniques to take control of literally millions of Windows machines around the world.

Tor aims to provide protection for ordinary people who want to follow the law. Only criminals have privacy right now, and we need to fix that. Some advocates of anonymity explain that it's just a tradeoff — accepting the bad uses for the good ones — but there's more to it than that. Criminals and other bad people have the motivation to learn how to get good anonymity, and many have the motivation to pay well to achieve it. Being able to steal and reuse the identities of innocent victims (identity theft) makes it even easier. Normal people, on the other hand, don't have the time or money to spend figuring out how to get privacy online. This is the worst of all possible worlds.

So yes, criminals can use Tor, but they already have better options, and it seems unlikely that taking Tor away from the world will stop them from doing their bad things. At the same time, Tor and other privacy measures can fight identity theft, physical crimes like stalking, and so on.

B Playing cards

In the workshop we presented the design choices as playing cards. These are included below to serve as reference as they are mentioned in the transcribed discussion. We used OpenAI's DALL·E for generating illustrative images.



Direct only 



DEFENSE Cannot be used for classic file-sharing and markets.

EFFECT Discovery and value for new-joiners -1.

INFO Messaging apps like Signal that require out-of-band connection are less likely to have grave social dynamics.

Index-search 



ATTACK Increases file-sharing use-case +2.

DEFENSE Resistance against node churning +1.

INFO Decentralised look-up protocols like DHT remove single-points of failure.

Following topics/people 



ATTACK Likelihood of spread of misinformation +1.

EFFECT Content discovery +1.

INFO Can lead to amplification of extreme voices as TikTok and Instagram showed.

Access to extern 



EFFECT +1 goodwill from the wider web.

EFFECT Availability of content and use-cases -1.

INFO Tor exit policies and the Tor exit node list are successful examples.

Alignment of trust 



EFFECT Deters all use-cases that do not align with the operator's values.

REQUIREMENT Can only be played with CUSTOM INFRASTRUCTURE.

EXAMPLE If the network is operated by a NGO, they will not protect illicit drug activities.