

On the anonymity “versus” accountability debate

Preface

Decreased privacy is an unavoidable consequence in the drive to make the world a more secure, safer place, according to some analysts [1]. In the on-line world, the conflict between privacy and security manifests itself in a debate between anonymity and accountability. This document seeks to examine this apparent dispute by describing the properties of anonymity and accountability in this context, presenting an instructive use case and extracting some insights in regard to the consequences for relevant stakeholders, should either of these two properties triumph over the other. At the end of this document, it is hoped that the reader will be better informed on this particular debate and, therefore, in a better position to make decisions about his/her on-line preferences and requirements.

1. Introduction

Anonymity and accountability are supposedly opposing factions in a zero-sum game between privacy and security. Conventional wisdom holds that decreasing anonymity (less privacy) is proportional to increasing accountability (more security). However, as Bruce Schneier, states,

“If you set up the false dichotomy, of course people will choose security over privacy -- especially if you scare them first. But it’s still a false dichotomy. There is no security without privacy.” [2]

In a similar vein, this document looks at the anonymity “versus” accountability debate and asserts that both characteristics can and must exist side-by-side in the on-line environment. Neither is enough on its own; and no person or organization should have to make a choice to use only one or the other.

2. Background

2.1. Anonymity

Anonymity refers to the absence of identifying information associated with an interaction [3]. On-line interactions can facilitate both more and less anonymity than those carried out in the physical world. Interpersonal transactions across the Internet allow greater anonymity at one level, but there is often an identifying data trail left by the Internet user. Such data can include names, dates-of-birth, credit card numbers, mailing addresses and buying patterns.

2.2. Accountability

An action is accountable if it can be attributed to someone (or something – such as a service provider – in this context). Accountability on the Internet is made possible by technical attributability. For example, associating a name/identifier to an IP address means that anyone sending malicious content from that location can be traced to that address. This is useful, since a lack of accountability generally means a lack of

incentive against bad behaviour. However, complete traceability/identifiability is also undesirable, as the ability to speak freely and without fear of oppression (i.e. probably anonymously) is a fundamental human right.

3. Use Case

The following scenarios give some context for the anonymity versus accountability debate:

Case 1

Alice is a student who puts up an anonymous web site with allegations that the President is a disgrace to the nation because he is a secret Anglophile.

Case 2

Alice is a student who puts up an anonymous web site with allegations that the President is a disgrace to the nation because he trades sex for Government positions.

Case 1 is surely worth anonymous protection, but *Case 2* seems to add weight to the belief that there should be increased accountability on the Internet.

However, the potential for abuse of power by traceability-seeking governments/administrators is much greater than that of an unidentified “ranting” user. Further, damage that is produced by an anonymous ranter can be controlled relatively easily by a government/administrator, in comparison to the difficulty which the anonymous ranter would have in trying to control the damage produced by an intrusive government. Thus, the balance between anonymity and accountability must be weighed on the side of the user’s anonymity.

This instance implies that the ability to remain anonymous in certain contexts should, therefore, be built into the future Information Society. With such a solid building block in place, the mechanisms to ensure accountability can then be pursued.

4. Two-tier Internet

The above use cases might be less ambiguous if a *secure* internet (accountable) and a “*free-for-all*” internet (anonymous) existed simultaneously. In this situation, the student, Alice, could use the appropriate identity – governmental, professional, consumer, whistleblower (anonymised), etc. – when posting her allegations. The weight of Alice’s allegations could then be measured against the strength of the identifier she uses when making the claims.

On the *secure* internet, the allegations might be taken seriously, as Alice would be required to reveal some identifying information before being allowed to post – thus, she would have opened a channel of redress for the defamed character in her claim. Conversely, on the “*free-for-all*” internet, where accountability is limited, the allegations would be akin to ranting alone in an empty room or in a room that no authority cares about and to which no one ever pays much heed. Such “*free-for-all*”

forums should not, however, become the equivalent of a sidelined ‘Speaker’s Corner’ [4]. To be walled inside a hermetically sealed environment, unable to be heard in the outside world, would not do justice to the rights of the political dissenter, for example.

5. Implementation

A strong theme to have emerged from Privacy Enhancing Technology (PET) research over the past few years is that anonymity/accountability properties have to be considered at both the transport (network) layer and application layer. If an anonymity property is not guaranteed at the transport layer, it could prove to be very difficult to simply “put back in” at the application layer.

There is also the issue of costs involved, when attempting to achieve either anonymity or accountability. This is especially pertinent in cases where the underlying transport layer does not support the respective feature.

If anonymity or unobservability is not supported at level $n-1$, then these properties become expensive to realize at level n . This is due to the need for establishing an *anonymity set* for every action; i.e. it is a recurring operational expense. This usually makes an activity much more expensive each time. For example, when trying to hide the direction of a message via dummy traffic, many (false) messages have to be sent, as opposed to just the one (true) message.

On the other hand, if accountability is not supported at level $n-1$, it does not seem to be as expensive as anonymity to realize at level n . There may well be a high one-time-cost to issue the identifiers needed for accountability. And there may be also some recurring costs involved in maintaining these identifiers, but this is not necessary for every transaction. The effort to “identify” transactions will not be as high as the cost of the respective transaction itself (unlike building an *anonymity set*, which is more expensive).

6. Conclusion

Anonymity is expensive to realize if the underlying network/transport layer does not have anonymity built in. Conversely, accountability is relatively easy and inexpensive to achieve if the underlying layer does not support anonymity. Thus, it may not be advisable to primarily focus on achieving accountability and then proceed to level everything down to achieve anonymity/unobservability; the other way round may prove to be more fruitful. It should be remembered too that just because accountability at the transport layer means that anonymity is nigh on impossible at the application layer today does not mean that this will be the case in the future.

What also needs consideration is the concept of non-binary anonymity; which is likely to be more prevalent in the future Information Society. Localised transparency/accountability (i.e. in a specific context) can lead to “graded” anonymity; thereby, increasing privacy outside of the local/specific environment.

Finally, it is worth recalling that the promises and guarantees given by service providers with regard to the confidentiality of users’ data are only as worthwhile as the governing authorities allow. If a future administration hinders such privacy, then today’s industry may well require systems for untraceable communications. This does not mean that everybody should be allowed to carry out transactions anonymously,

but it does support the point for essentially anonymous communication infrastructures, on which one can build traceability.

References

- [1] <http://arstechnica.com/security/news/2008/01/us-intel-chief-wants-carte-blanche-to-peep-all-net-traffic.ars>
- [2] http://www.schneier.com/blog/archives/2008/01/security_vs_pri.html
- [3] Nissenbaum, H, “*The meaning of anonymity in an information age*”, **Inform. Soc.** **15 (1999)**, pg. 141–144.
- [4] http://en.wikipedia.org/wiki/Speakers%27_Corner

Acknowledgement

This article is based on discussions between members of the Think-Trust project Work Groups. For more information see www.think-trust.eu or contact bfoley@tssg.org.