D64

Zentrum für
Digitalen Fortschritt

The Login-Trap: Combating Hate Speech without Mass Surveillance

D-64.ORG

The Login-Trap: Combating Hate Speech without Mass Surveillance

Hate crime on the Internet is a problem: Women and marginalized groups in particular, who are also vulnerable to harassment and discrimination "in the analog world," are insulted and threatened on the Internet every day. In some of these cases, offenders use the cloak of anonymity in an attempt to escape consequences for their criminal actions.

Anonymity on the Internet is important. It protects many people who do good but have to fear reprisals: be they journalists, whistle-blowers or opponents of regimes in authoritarian states.

Much like the secrecy of the ballot when voting in elections, anonymity can be key for a free expression of opinions. In particular people who are in weaker positions in the social hierachy depend on this protection.

For this reason, anonymity on the Internet must be preserved as a matter of principle. Nevertheless, an effective instrument for law enforcement is needed. Our proposal: the login-trap.

Not the answer: Obligation to use real names and identification

Mandatory real name and identification requirements, which keep popping up in the political debate, are therefore not a good idea. With a real-name obligation, every person who is active in a social network must publicly display his or her "real", legal name. Such an obligation will in particular restrict the factual possibilities of expressing opinions of people who are particularly worthy of and in need of protection. These are people in relationships of dependency who would have to fear repression in their social and professional environment when being required to use their real name online. In addition, the obligation to use ones real name eases stalking and personal threats, because offenders would have access to the personal data of potential victims, which can be used, for example, to find out their address or other contact information.

Consequently, this measure does not counter hate crime but makes it easier to commit more serious subsequent crimes.

This argument does not apply equally to an identification obligation, where the data is "only" stored by the platforms, but it remains possible to act with pseudonyms in the public. Nevertheless, vast amounts of verified personal data are stored by private organizations, making the companies (even) more attractive for cyber attacks. An example from South Korea shows that this danger has already become reality: With a comparable solution in place, data from 35 million citizens was stolen. In addition, the recent criticism of Whatsapp's new privacy policy shows that many citizens are (rightly) unwilling to share even more private information with the leading social networks, which are not known for their data protection friendliness.

Our solution: The login-trap

We believe that effective law enforcement online is already possible with the existing legal toolbox in Germany. Without the additional storage of data and without new legal powers transferred to law enforcement, the de-anonymization of suspects can work if law enforcement agencies, platforms and telecommunication providers standardize their communication and data exchange.

We propose the following procedure when - as an example - Olivia is insulted and threatened by the user "Teddy Bear" on Facebook:

1. Olivia reports the post **directly on the platform to the responsible I** via a simple, user-friendly interface. The **offending post is immediately transmitted** to law enforcement agencies without the need for manual screenshots or the like.
2. Trained police officers or prosecutors check the report, **confirm initial suspicion** and **set up the "login-trap"** for "Teddy Bear" on Facebook.
3. The Facebook app on "Teddy Bear's" smartphone either **connects** in the background (as it does regularly) or "Teddy Bear" **actively opens Facebook** in a browser to look at new posts.

4. The **login-trap snaps**: At short notice (favorably in real time), the **IP address of "Teddy Bear"**, with which the renewed login takes place, is transmitted to the responsible investigating authority.
5. The investigating authority forwards the IP address to the **responsible telecommunications provider** and receives the stored **personal details** (name and address) from them.
6. "Teddy Bear" is **successfully identified**, charges can be filed.

The legal basis for these investigative measures already exists – at least in German law: Law enforcement agencies are entitled to query IP addresses and personal details, and the platform and telecommunications providers are obliged to hand over the data. In practice, however, investigations often fail because they are not carried out with the necessary urgency, so that the digital traces are becoming worthless. The solution cannot be to oblige private companies to retain data for long periods of time or to use other instruments to monitor citizens *en masse* without specific reasons. Instead, investigative methods must be developed that are sufficiently fast and require action only after initial suspicion has been established.

For such a measure, an agreement on standardized APIs between investigative authorities and social networks. Using these APIs, both the requests for personal data and the transmission of such data can take place securely and quickly. Sending faxes and manual e-mails hinders the effective prosecution of crimes and is ineffective, with no advantages from the standpoint of data protection. Instead, these shortcomings lead to demands such as bulk data retention and mandatory identification, which are disproportionate, not least because better alternatives have been demonstrated.

Freedom needs security

Security and freedom are not opposites. Only those who feel safe can be free. But security is of no value if it does not guarantee freedom. That is why effective law enforcement is needed in the field of hate crime, so that freedom of expression can be guaranteed for the groups that are particularly affected by insults and threats.

Security, however, is not an end in itself. In a free, democratic society, the principle must always be the absence of surveillance.

Government tools like data retention reverse this principle, tools like the German “state Trojan” promote the existence of insecure IT infrastructure.

As an alternative, our login-trap is meant to be a proposal for how effective law enforcement can be carried out without mass surveillance, also in the digital space.

IMPRINT

ABOUT D64

D64 is the center for digital progress.

D64 is the center for digital progress. We see the digital transformation as a great opportunity to improve our common bond in modern society. We want to influence social, ecological, technological and political development constructively, critically and creatively.

Our goal is to realize the fundamental values of freedom, justice and solidarity through a progressive digital policy. To this end, we act with the help of the wide-ranging expertise of our more than 700 members as an independent association pioneering and providing impetus in all areas of digitization.

d-64.org

CONTRIBUTION

This idea was developed in an internal working process at D64 by Henning Tillmann and Erik Tuchtfeld.

MORE LANGUAGES

A German version of this paper can be found on https://d-64.org/login-falle.

ADDRESS

D64 – Zentrum für Digitalen Fortschritt e.V.
Co-Chairman: Henning Tillmann
Co-Chairwoman: Marina Weisband
Gipsstr. 3
10119 Berlin

CONTACT

Erik Tuchtfeld
Member of the Board

erik.tuchtfeld@d-64.org

November 2021