INIT

Pseudonimity and Anonymity as Tools for Regaining Privacy

We are living what has been purported as the newest industrial-like revolution for online services and telecommunications.

We have now reached a point where the majority of people rely solely on the internet for communication, geographical navigation, entertainment, socialization (be it via social networking sites, email, or other communication forms), education, research, accounting, consultancy, and a plethora of other activities and processes. As this may be perceived as a positive development, the increase of internet penetration worldwide comes with a vast industrial concentration that makes surveillance, censorship, unjustified control, and exploitation of personal or otherwise sensitive data effortless.

Since the 1990s, companies have tried to monopolize the online market by offering all kinds of free services, including but not limited to websites, email, file storage, chat, voice communication, discussion forums, and collaboration platforms. Maintaining a large-scale service requires significant technical resources (hardware, servers, and network and electrical infrastructure) and human resources (developers, user support, and all the other people who work around the clock to keep these services running), which raises the question: How can all of these services be offered free of charge? The answer is data.

With large acquisitions of user data and personal information, companies have been directly (or indirectly) selling your personal information to advertisers, marketers, researchers, and pretty much anyone who can pay. Many companies have become desperate for market monetization and control, to extreme points often seen as immoral. Some will trade and sell health data, infiltrate and hack users' devices to gain access to their local storage, record audio and video conversations, use location tracking and logging, save search results, scour calendar items, store uploaded content (such as photos, videos, and files), and install applications on pretty much everything we use in our personal and business workspace environment.

Additionally these companies will cooperate with any federal or governmental entities, and will hand over data and personal user information without any consent from or notification of their clients and users. This should not be surprising when many tech companies have developed systems and advanced programmatic interfaces that are tailored to ease governments and federal entities acquiring user data.

Many companies will go far as possible to maintain their market position by acquiring or buying out smaller (often innovative) businesses, only to then close them down in order to erode competition or to acquire their patents. Quoting Richard Stallman, founder of the Free Software Foundation and a strong online privacy advocate, "There are so many ways to use data to hurt people that the only safe database is the one that was never collected" [1].

For this issue, we invited a number of people who are trying in their own way to alter, hinder, and fix current internet defaults—mass surveillance, oligopoly, and censorship—either by technical developments or policy changes, social movements, and politics. We strived to present a set of authors who "get their hands dirty." Implementors, if you will, of the technologies presented, rather than people deeply involved in academia.

Big data and power concentration threaten the internet.

You will find eight very different feature articles, some written individually and some collectively. We hope you enjoy reading this issue as much as we have enjoyed bringing these wonderful authors together.

The topic of privacy, anonymity, and pseudonymity is difficult to understand and needs a gentle introduction. "Demistifying the Dark Web" opens the discussion by presenting the technical foundations for anonymizing networks and a brief discussion on how the popular Tor network is implemented. Anonymization networks have often been demonized by the press, which coined and continues to misuse the term "dark web." The truth of this claim is also brought up for discussion: What really lives hidden under the layers of the onion?

"Autonomous Infrastructure for a Suckless

Across the globe, 60 percent of internet users only have access to a censored internet.

INIT

Internet" provides a timeline on the emergence and the role of autonomous internet infrastructures with respect to their operation and connection to social struggles based on a 10 year-long qualitative analysis of autonomous infrastructure. Stefania Milan's article sets out working "examples of alternative modes of organization, closer and fairer relationships between infrastructure operators and users, and novel responsibilities toward the latter." She touches upon community wireless and cellular networks, bulletin board systems, internet cables, and grassroots internet service providers (ISPs),

The underlying network protocols of the internet's current architecture were not designed with privacy in mind, assuming "network operators had no interest in the data they were carrying," which we now know was an invalid assumption according to Jack Grigg. In his article, "The Principle of Least Authority," Grigg describes how development centers around the idea of capabilities—"the ability to ensure privacy of both our content and metadata in a decentralized manner"—and how (if possible) this could be applied to the entire internet.

"Routes to Rights" urges greater emphasis on the impact that network protocols and technical infrastructure has in our lives. Backward compatibility and legacy with older versions of the current internet infrastructure make innovations, problem fixes, and developments hard to apply or utilize, and usually remain unaddressed in newer protocol versions and infrastructures. Furthermore, authors Niels ten Oever and Davide Beraldo describe the centralization of ownership and how some oligopolies force decisions that affect network protocols and software development decisions.

Kali Kaneko's "Stop Looking Over Our Shoulders!" focuses on the global concern of the "digitization of everything—from newspapers to protest" and how people began to recognize the problems of the today's internet. The article highlights the importance of obfuscating our online identity and activities, pseudonimity, and the crucial function of cryptography. All of which are still effective countermeasures against massive advertisement tracking and online identity protection.

"How to Fix Email" presents a proposal for better email transit. Although email has been declared dead multiple times, federated email servers keep relaying messages (emails) for around 3 billion users, forming the largest open federated message transport system. Holger Krekel, Karissa McKelvey, and Emil Lefherz present how a diverse group of developers, hackers, and researchers attempted to fix email encryption—a decades old technology that is not widely adopted, due to its usability issues and the fact that a limited group of entities use it.

The privacy options and technologies around a crucial software component of the World Wide Web, the web browser, are evaluated in "Can We Build a Privacy-Preserving Web Browser We All Deserve?" Christoph Kerschbaumer, Luke Crouch, Tom Ritter, and Tanvi Vyas describe the benefits and drawbacks of each privacy enhancing feature of web browsers and assess "the capabilities of web features to find the right balance between enhanced experiences for the web, while also preserving user privacy." A hard task that often devolves in trial and error practices or lessens user experience, as many websites may not be fully functional.

carlo von lynX's "The Case for Regulating Social Networks and the Internet" depicts how big data and power concentration threaten the internet. He provides some political and legislative proposals for the next-generation internet that will not manipulate but treat citizens equally, and not infringe on the capacity of citizens to freely form their political opinions. The author describes how proposed changes—mandatory end-to-end encryption, data tracking collection hindering, metadata protection, anonymity, and telephony without location tracking—can help regain liberty online.

The editors want to acknowledge the UNAM/DGAPA/PE102718 project for supporting the time vested in preparing this issue of *XRDS*.

References

[1] Stallman, R. A radical proposal to keep your personal data safe. *The Guardian* (April 3, 2018); https://www.theguardian.com/commentisfree/2018/apr/03/facebook-abusing-data-law-privacy-big-tech-surveillance

—Vasilis Ververis and Gunnar Wolf

DOI: 10.1145/3220575