Cryptography is Important to the Public Interest

This is a joint letter to the UN Special Rapporteur on Freedom of Expression from the undersigned non-governmental organizations in response to his January 2015 request for comments on encryption, anonymity, and online security.

We ship cryptography for the public good

As developers, facilitators, and distributors of free and open source software, we include cryptographic tools and mechanisms in the tools we provide to the public.

Examples of Free and Open Source software with cryptographic tools and mechanisms include:

- Web browsers like Firefox and Chromium and GNOME Web and web servers like Apache httpd and nginx – these use cryptography to enable users to have authenticated, confidential communications to web sites.
- Operating system kernels like Linux and the FreeBSD kernel – these use cryptography to provide users with confidential data storage and network communications.
- Database engines like MySQL and PostgreSQL and administration programs for them such as phpMyAdmin – these use cryptography to provide authenticated connections to databases, to restrict data to only those authorized to see it, and to protect the contents of database queries in transit.
- E-mail programs like Thunderbird and Evolution – these use cryptography to provide confidential E-mail transport, as well as end-to-end confidential messages over e-mail.
- Chat programs like Pidgin and Jitsi – these use cryptography to provide confidential instant message transport, as well as end-to-end conversation privacy (including "off the record" messaging).
- Encryption toolkits like GnuPG, OpenSSL, GnuTLS, and NaCl – these cryptographic toolkits enable other projects to provide secure communication, data storage, and verifiable signatures.
- Secure communications tools like OpenSSH and OpenVPN, which allow confidential connections between systems.
- Programming languages like Python and Ruby – these systems of expression in computer code include libraries (programmatic building blocks) that provide cryptographic functions for people who write programs in them.

While not every piece of free software uses cryptography directly, many do, and even non-cryptographic software often relies on cryptographic software to perform its intended function.

We rely on cryptography for our internal processes

In addition to providing cryptographic tools for the greater good, we rely on those tools internally for our organizations to function effectively. Our organizations are geographically diverse, and we rely on strong, secure communications both for members' internal communications and workflows, and for our public-facing presence on the Internet.

Collectively, our organizations use a variety of technical systems, including mailing lists, revision control software, instant message chat systems, remote computer access ("shell accounts"), bug reporting tools, project planning systems, and voting mechanisms. All of these systems rely on strong cryptography in some way to ensure that our work goes as planned, that confidential discussions can be had where needed, and that decisions taken on behalf of the organization are made by the appropriate people. Without cryptographic tools, our organizations would be unable to securely provide or administer internal organization services.

Software Contributions

When software is contributed by an organization member or an associated volunteer, we can use cryptographic means as part of the process to decide whether to include or accept the contribution. Without cryptographic signatures, we would have only weaker mechanisms to protect against counterfeit or spoofed submissions.

Software Distribution

When we distribute software or source code to the public, our (often anonymous) users rely on cryptography to ensure that the software or source code they're receiving actually came from us. This is critical to establishing trust, building a solid reputation, and providing reliable service to the communities we aim to serve. Without cryptographic tools, our users (indeed, all users who fetch any software over the Internet) would have no choice but to accept updates and to reveal the set of software they have installed to whoever controls their network access.

Public Feedback

When we accept reports of problems or suggestions for improvements from our membership or the general (sometimes anonymous) public, we rely on cryptography to ensure that the reports and suggestions are confidential when they need to be, and can be followed up on in confidence. Not all such reports or suggestions need to be confidential, but some are sensitive, and need to be handled securely. Without encryption, we would be unable to provide these confidential channels, which would limit our ability to improve the tools we offer to the public.

Cryptography is a requirement for people to control their own communications

We provide and rely on these cryptographic tools because people are entitled to fundamental control over their communications. A global communications network without these tools would be an unthinkable tragedy: the users of the network would be subject to the whim of the operators of the network, or to whoever can control or coerce the network operators.

People need to be able to have secure, confidential, private communications for many reasons: as entrepreneurs and businesspeople; as political beings, organizers against injustice and repression; as individual humans for personal and social development; as members of nation states exercising sovereignty; and as partners in diverse global projects, building systems together without interference.

There are many actors who aim to break these systems, to overpower people by controlling or snooping on their communications. These actors include rival businesses conducting industrial espionage; repressive nations acting against their own citizens; abusive partners, family, bosses, and employees; antagonist nation states jockeying for domninance; common thieves and organized crime; and anyone threatened by the free flow of ideas and information.

Cryptographic tools offering privacy, anonymity, confidentiality, and authenticity are necessary (but not sufficient) to support this fundamental human right.

Support encryption and anonymity

As organizations constituted to benefit the public good, we facilitate the development and distribution of tools that help people to control their communications, to hide or proclaim their public identity as they see fit, and to guard over their private information. Cryptography is today a critical part of that promise.

We urge the UN and other governmental bodies to support us and to support the public in these goals by recognizing cryptography and anonymous communications as fundamental precursors to the rights of freedom of expression, association, and privacy.

Endorsed By:

- The OpenSSL Project `https://openssl.org/`
- Free Software Foundation `https://fsf.org/`
- Association for Progressive Communications `https://apc.org/`
- Fantsuam Foundation `http://fantsuam.net/`
- The LEAP Project `https://leap.se/`
- Software Freedom Conservancy `https://sfconservancy.org/`
- GNOME Foundation `https://www.gnome.org/foundation/`