

# Cypherpunkts und Privatsphäre

- Prof. Dr. Florian Tschorsch
- Cypherpunks
  - Was sind Cypherpunks?
  - Wie hat sich die Bewegung entwickelt?
  - Wichtige Personen und Projekte
- Forschungsfrage

- Informatik-Studium an der Heinrich-Heine-Universität Düsseldorf
- Promotion an der Humboldt-Universität zu Berlin in 2016
- Seit 2017 Juniorprofessor an der Technischen Universität Berlin
- Forscht an anonymer Kommunikation und Blockchain



Quelle: [https://pbs.twimg.com/profile\\_images/824000575083790340/hclYN\\_4Q\\_400x400.jpg](https://pbs.twimg.com/profile_images/824000575083790340/hclYN_4Q_400x400.jpg)

A person who uses encryption when  
accessing a computer network  
in order to ensure privacy,  
especially from government authorities.

(laut Oxford Dictionary [<https://en.oxforddictionaries.com/definition/cypherpunk>])

# Einwurf: Privatsphäre

- Begriff verwirrt oft als das er beschreibt
- Am besten als „shorthand umbrella term“ benutzt
- „Der Bereich, in dem eine Person selbst bestimmt [...], wem sie wann und warum welche Information über sich selbst zugänglich macht“

# Einwurf: Geheimhaltung

- „Ein Geheimnis ist eine meist sensible Information, die einem oder mehreren Eigentümern zugeordnet ist“
- Aufbewahren von Geheimnissen, damit diese nicht in fremde Hände geraten

# Cypherpunk Manifest

- Privatsphäre ist wichtig für offene Gesellschaft
- Privatsphäre  $\neq$  Geheimhaltung
- Werkzeuge: Anonyme Transaktionssysteme & Verschlüsselung
- Jede Person muss eigene Privatsphäre verteidigen
- Cypherpunks schreiben Code für eigene und Privatsphäre anderer
- Wichtig: Gesellschaft muss sich auf Privatsphäre als allgemeines Gut einigen

# Kleine Geschichtsstunde



„Household Cavalry Regiment Scout 3 on Salisbury Plain“ via [Wikimedia Commons](#), licensed under [CC-BY-NC-SA](#)

[Back to article on net.cabernik.com](#)

### A Cypherpunk's Manifesto

by Eric Hughes

Privacy is necessary for an open society in the electronic age. Privacy is not secrecy. A private matter is something one doesn't want the whole world to know; but a secret matter is something one doesn't want anybody to know. Privacy is the power to selectively reveal oneself to the world.

If two parties have some sort of dealings, then each has a memory of these dealings. Each party can speak about their own memory of this, how could anyone prevent it? One could pass laws against it, but the freedom of speech, even more than privacy, is fundamental to an open society; we seek not to restrict any speech at all. If many parties speak together in the same forum, each can speak to all the others and aggregate together knowledge about individuals and other parties. The power of electronic communications has enabled such group speech, and it will not go away merely because we might want it to.

Since we desire privacy, we must ensure that each party to a transaction have knowledge only of that which is directly necessary for that transaction. Since any information can be spoken of, we must ensure that we reveal as little as possible. In most cases personal purchase is required as a store and hand each to the clerk, there is no need to know who I am. When I ask my electronic mail provider to send and receive messages, my provider need not know to whom I am speaking or what I am saying or what others we expect know how to get the message there and how much I owe them in fees. When my identity is revealed by the underlying mechanism of the transaction, I have no privacy. I cannot here selectively reveal myself; I must always reveal myself.

Therefore, privacy in an open society requires anonymous transaction systems. Until now, cash has been the primary such system. An anonymous transaction system is not a secret transaction system. An anonymous system empowers individuals to reveal their identity as they desire; this is the essence of privacy.

Privacy in an open society also requires cryptography. If I say something, I want it heard only by those for whom I intend it. If the content of my speech is available to the world, I have no privacy. To encrypt is to indicate the desire for privacy, and to encrypt with one who trusts desire for privacy. Furthermore, to read one's identity with assurance when the default is anonymity requires the cryptographic signature.

We cannot expect governments, corporations, or other large, faceless organizations to grant us privacy out of their benevolence. It is to them all wrong to speak of us, and we should expect that they will speak. To us to prevent this speech is to fight against the power of the state, and it is to be free, it is to be free. Information expands to fill the available storage space. Information is Ramon's younger, stronger cousin; Information is Esther of East, has more eyes, knows more, and understands less than Ramon.

We must defend our own privacy of we expect to have any. We must come together and create systems which allow anonymous transactions to take place. People have been defending their own privacy for centuries with whippers, barbed wire, entrapments, closed doors, and other means. The technologies of the past did not allow for strong privacy; but electronic technologies do.

We the Cypherpunks are dedicated to building anonymous systems. We are defending our privacy with cryptography, with anonymous mail forwarding systems, with digital signatures, and with electronic money.

Cypherpunks write code. We know that someone has to write software to defend privacy, and since we can't get privacy unless we all do, we're going to write it. We publish our code so that our fellow Cypherpunks may practice and play with it. Our code is free to all, much care if you don't approve of the software we write. We know that software can't be destroyed and that a widely dispersed system can't be shut down.

Cypherpunks declare regulations on cryptography; for encryption is fundamentally a private act. The act of encryption, in fact, removes information from the public realm. Even laws against cryptography reach only so far as a nation's border and the area of its jurisdictionally spread over the whole globe, and with it the anonymous transaction systems that it makes possible.

For privacy to be widespread it must be part of a social contract. People must come and together deploy these systems for the common good. Privacy only extends so far as the cooperation of one's fellows in society. We the Cypherpunks seek your questions and your help so that we do not become cowards. We will act, however, be named out of our course because some may disagree with our goals.

The Cypherpunks are actively engaged in making the networks safer for privacy. Let us proceed together again.

Overend:

Eric Hughes [shughes@unix.berkenc.edu](mailto:shughes@unix.berkenc.edu)

9 March 1993

A flyer for a CryptoParty in Santiago, Chile, featuring Alice in Wonderland imagery. The flyer has a pink and black color scheme. On the left, a purple box contains the text: "VUELVE SEGURAS TUS COMUNICACIONES Y DEJA A LA REINA DE CORAZONES CON TRAGEDIA cryptopartycl". In the center, a white rabbit and Alice are depicted. On the right, a pink box contains the text: "¿CUÁNDO? 28 SEP. 20:00 hrs. CASA VOLNITZA Vidaurre 1629, Santiago centro. ¿MÁS INFO? cryptoparty.org". At the bottom, a pink box contains the text: "¿QUÉ HAREMOS? Nos reuniremos para enseñar, compartir y aprender las herramientas esenciales para la supervivencia en la red. tales como PGP/GPG, Tor, OTR, TrueCrypt, etc. ¿Retención de datos? ¿Intercepción de mensajes? ¿Acoso?... HAGAMOSLES LA PEGA MÁS DIFÍCIL QUE LA CHUCHA." There are also several blocks of encrypted text (PGP messages) scattered throughout the flyer.

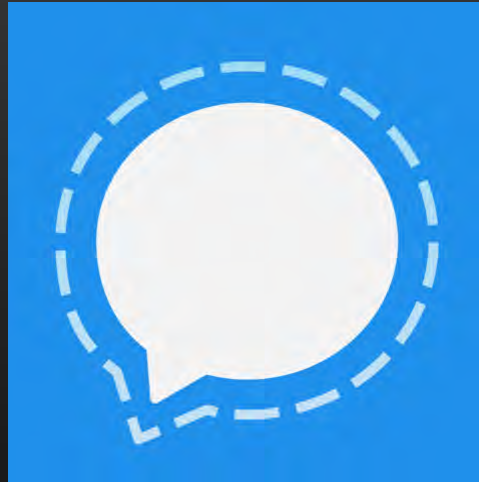
„A flyer for a CryptoParty in Santiago, Chile using Alice in Wonderland imagery“ by Santiago Cryptoparty, licensed under [CC-BY 3.0](#)



# Einige wichtige Projekte



„Tor logo“ by [The Tor Project, Inc.](#),  
licensed under [CC BY 3.0 US](#)



[https://github.com/WhisperSystems/Signal-iOS  
/blob/master/Signal/iTunesArtwork%403x.png](https://github.com/WhisperSystems/Signal-iOS/blob/master/Signal/iTunesArtwork%403x.png)



„New bitcoin logo“ by Bitboy,  
licensed under CC0

# Einige wichtige Personen



Bild: Wikipedia / Tobias Klenze / [CC-BY-SA 4.0](#)



„Moxie Marlinspike“ by [Knight Foundation](#),  
licensed under [CC-BY-SA 2.0](#)

Satoshi Nakamoto

Eric Hughes

Ich habe doch nichts zu verbergen!

# Weiterführende Links

- Seite von Prof. Dr. Florian Tschorsch (<http://www.dsi.tu-berlin.de/menue/arbeitsgruppe/tschorsch/>)
- Cypherpunk Manifest (<https://www.activism.net/cypherpunk/manifesto.html>)
- Englischer Wikipedia-Artikel zu Cypherpunks (<https://en.wikipedia.org/wiki/Cypherpunk>)
- Spiegel Online Artikel zu Cryptopartys (<http://www.spiegel.de/netzwelt/netzpolitik/cryptoparty-bewegung-die-cypherpunks-sind-zurueck-a-859473.html>)

# Weitere Quellen

- <https://en.oxforddictionaries.com/definition/cypherpunk> (zuletzt abgerufen am 13.12.2017)
- <https://twitter.com/flotschorsch> (zuletzt abgerufen am 13.12.2017)
- <https://de.wikipedia.org/wiki/Geheimnis> (zuletzt abgerufen am 13.12.2017)
- Solove, Daniel J., 'I've Got Nothing to Hide' and Other Misunderstandings of Privacy. San Diego Law Review, Vol. 44, p. 745, 2007; GWU Law School Public Law Research Paper No. 289. Available at SSRN: <https://ssrn.com/abstract=998565>

# Weitere Quellen (Fortsetzung)

- Prof. Dr. Lutz Prechelt: „Vorlesung Anwendungssysteme: Privatsphäre“