



# **Anomos**

Applied Cryptography and Human Rights

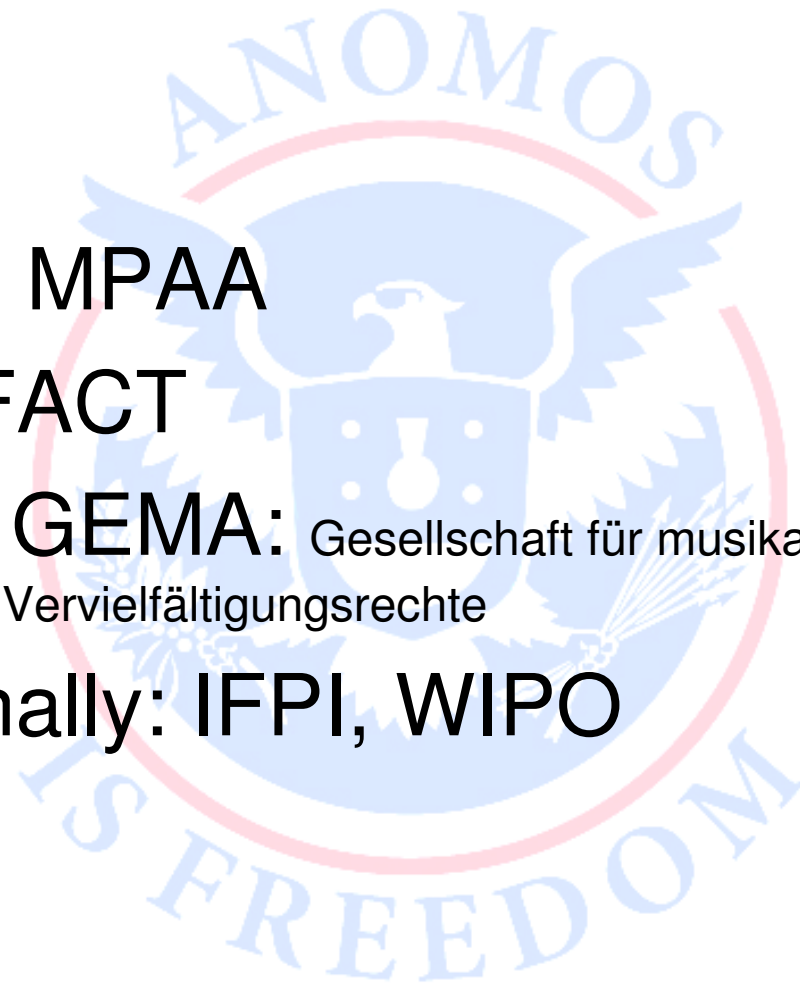
by: Rich Jones, John Schanck

# Historical Primer

- “And just as a seemingly minor invention like barbed wire made possible the fencing-off of vast ranches and farms, thus altering forever the concepts of land and property rights in the frontier West, so too will the seemingly minor discovery out of an arcane branch of mathematics come to be the wire clippers which dismantle the barbed wire around intellectual property.
- **Arise, you have nothing to lose but your barbed wire fences!”**
- - Tim May, *The Crypto-Anarchist Manifesto*
  - Tim later became a Chief Scientist at Intel

# IP: The Usual Suspects

- US: RIAA, MPAA
- UK: BPI, FACT
- Germany: GEMA: Gesellschaft für musikalische Aufführungs- und mechanische Vervielfältigungsrechte
- Internationally: IFPI, WIPO



# Evil

- Corporations are pressuring (corrupting) governments to regulate the internet to protect their ability to restrict our access to information (DMCA/EUCD/EIPA)
- Specifically targeting young people with lawsuits
- Killing our right to Fair Use

# Beyond IP: Worse than Evil

- Domestic Surveillance
- NSA Wiretaps
- Proposed UK Email Record Database
  - <http://news.bbc.co.uk/2/hi/technology/7410885.stm>
- Attempts in Sweden
- China

# Rights Lost

- This violates our rights to
  - Privacy
  - Access To Information
  - Free Speech and Self Expression
- This is akin to **Mind Control**
  - This is very very bad.
- This leads to the erosion of other rights
- The solution!:

# Cryptonymity!



# The solution!

- Cryptonymity!
  - That's not a word
    - Yet
- Combination of cryptography and anonymity
- They can't know who we are or what we are doing
- This is the only true freedom

# What is Anomos?

- Anomos is an encrypted, pseudonymous multi-peer-to-peer file sharing protocol, based on BitTorrent.
- The current code in the git repository is based of a fork of the official BitTorrent tracker/client, version 4.0.
- Supported by



# What pros and cons of BitTorrent?

- + FAST (Multi-peer2peer, as opposed to old, directly connected p2p such as Napster).
- + Widely Used
- - Unencrypted
- - Onymous
- - Traffic is deliberately sniffed by companies playing detective, such as MediaSentry
- - This means that users can be tracked, and some will be prosecuted.
- - Traffic may be tampered with by ISPs

# What are the pros and cons of current encryption/routing schemes?

- + Routing traffic is encrypted
- +/- Encrypted traffic (and unencrypted traffic without identifiable information) is pseudonymous
- - Less widely used
- - Typically slow(er)
- - Blocking/discouragement of P2P

# How does Anomos work? (Not too technically..)

- The file being transferred is encrypted with 256-bit AES.
- The pseudonymity is provided by a routing mix network, which has SSL encrypted peer to peer links.
- The protocol still requires the presence of a trusted tracker, who handles calculating the data paths.

# What are the pros and cons of Anomos?

- +Encrypted end to end
- +Pseudonymous Mixnet
- +Fast speeds of Multi-P2P (Though not as fast as normal BT)
- +Based on popular, familiar technologies
- -Use of a centralized tracker

# Reasons



- Liu Tao
- [http://www.ananova.com/news/story/sm\\_1399668.html](http://www.ananova.com/news/story/sm_1399668.html)
- Expose worse corruption and negligence
- The rise of citizen journalism

# Citizen Journalism

- With Anomos, there can be anonymous news outlets who can report without fear of any repercussions for transmitting material
- Censorship Resistant Media
- Viewers/Readers are also safe to receive materials
- WikiLeaks, LiveLeak, Miro

# Right to Information

- Safe access to religious or sexual material in repressive Islamic countries
- China: Information about Tiananmen Square or that criticizes the government
- Software used for digital artistic and intellectual expression.
- And, yes, digital media.

# Cryptoanarchizing Tools

- A lot of people have talked about the internet as a 'democratizing' tool.
- But, they have seemed to missed the point.
- Rather, the internet is a brilliant ***anarchizing*** tool, as no power has to be relented to anybody in order to spread any type of information.
- Anomos ensures this in a practical sense.

# Help Wanted!

- We need help!
- This is an open-source project and we are looking for any developers who are interested to come and contribute code
- or help test the security of the platform.
- Also, of course, we need kind souls to run some trackers! (Swedes wanted.)

# More info

- Website: <http://www.anomos.info>
- Git: <http://anomos.info/git/>
- Rich: **[rich@anomos.info](mailto:rich@anomos.info)**
- John: **[john@anomos.info](mailto:john@anomos.info)**
- To help: [participate@anomos.info](mailto:participate@anomos.info)

