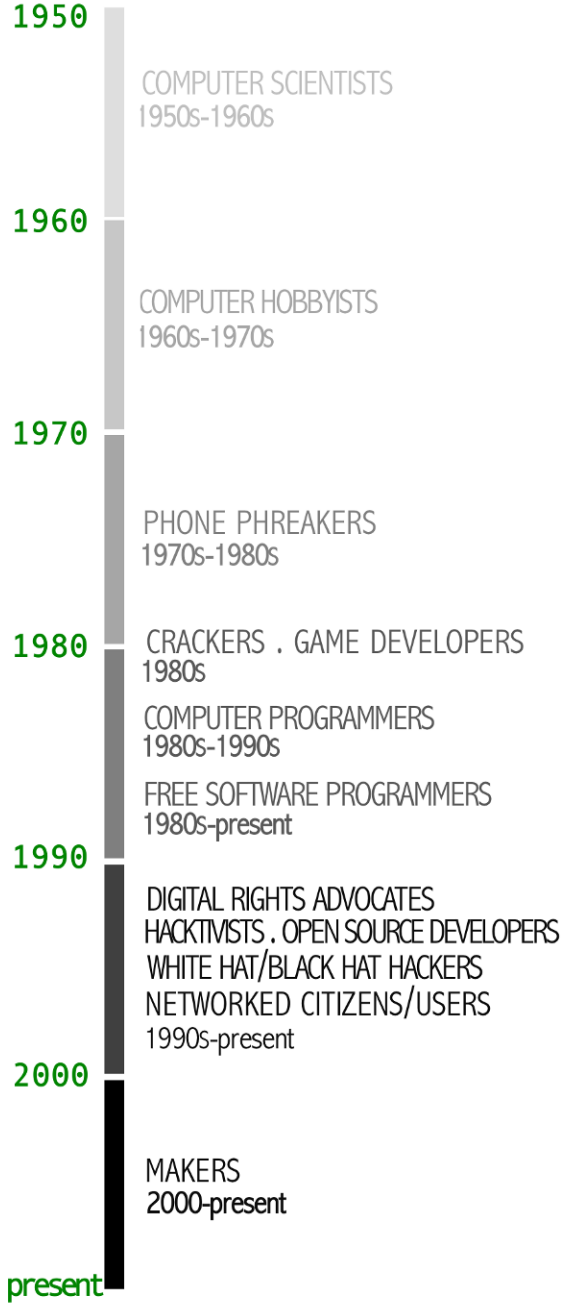
IT wants to be freed:

Hackers and the evolution of technology regulation

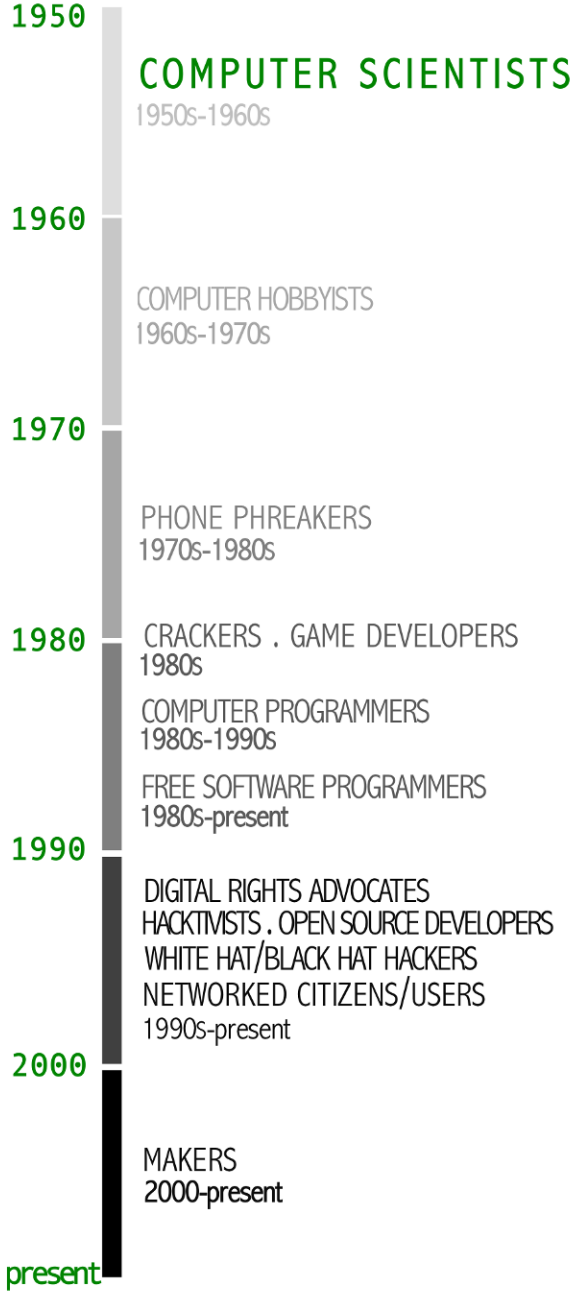
Michael Dizon

Hackers



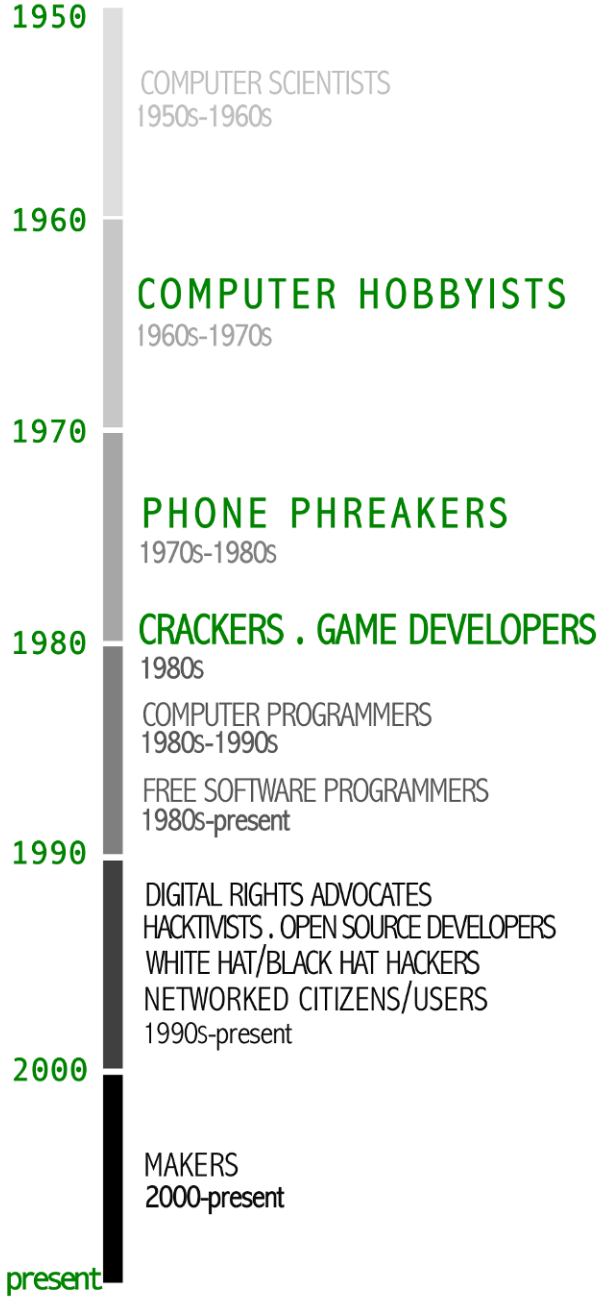
Who are hackers

- Not one but many types
- A loosely-joined but distinct hacker culture



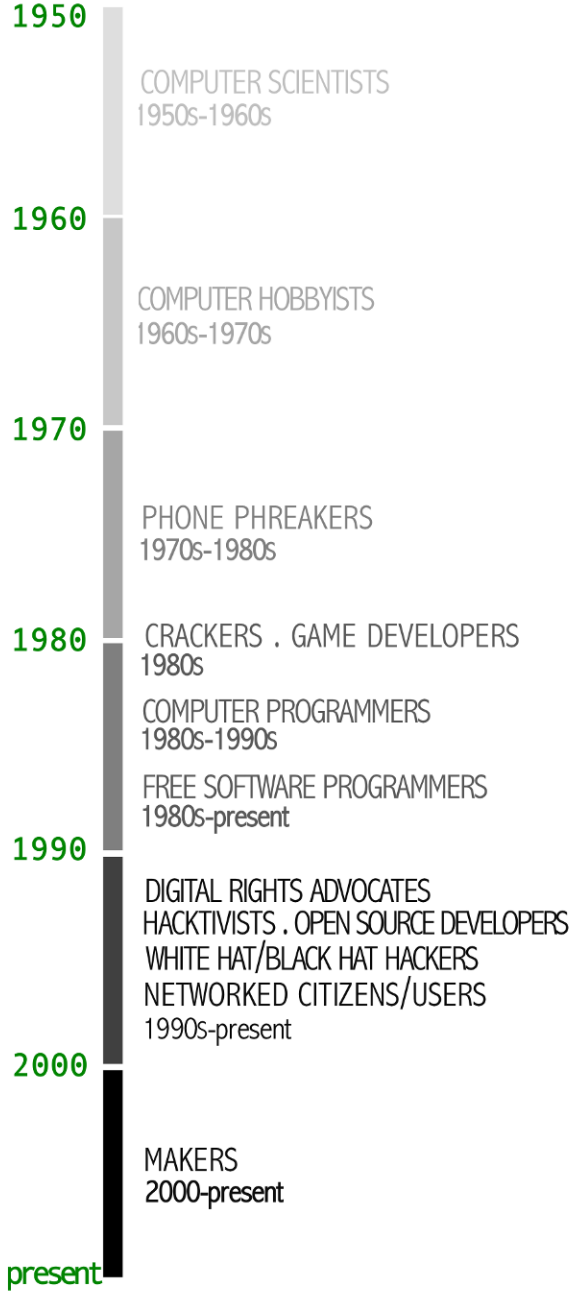
Hacker ethic

- Early hacker ethos:
  - Free access to computers
  - All information should be free
  - Mistrust authority – promote decentralization
  - Judged for technical skills and achievement
  - Create art and beauty on a computer
  - Computers can change your life for the better
- Not subject to direct state regulation



Hacker manifestos

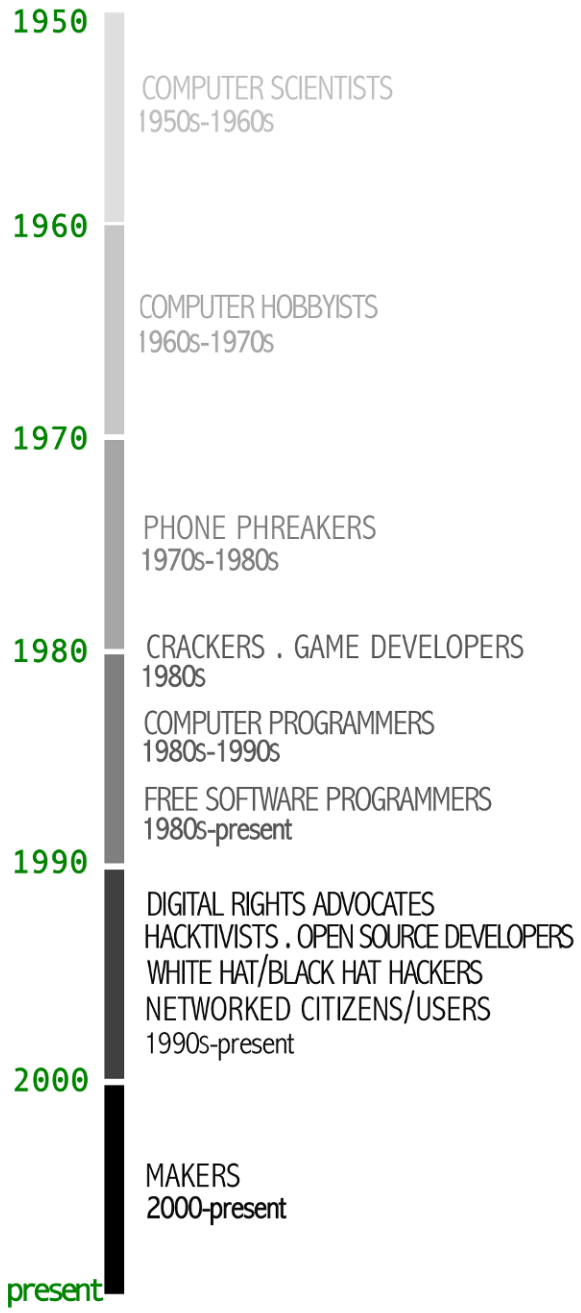
- Demonisation and FUD
- Jargon File and Hacker's Dictionary
  - Information sharing
  - Fun and exploration but no damage
- The Hacker Manifesto
  - Free service
  - Explore and seek knowledge
  - Curiosity
  - Judged by words and actions



Hacker norms & values

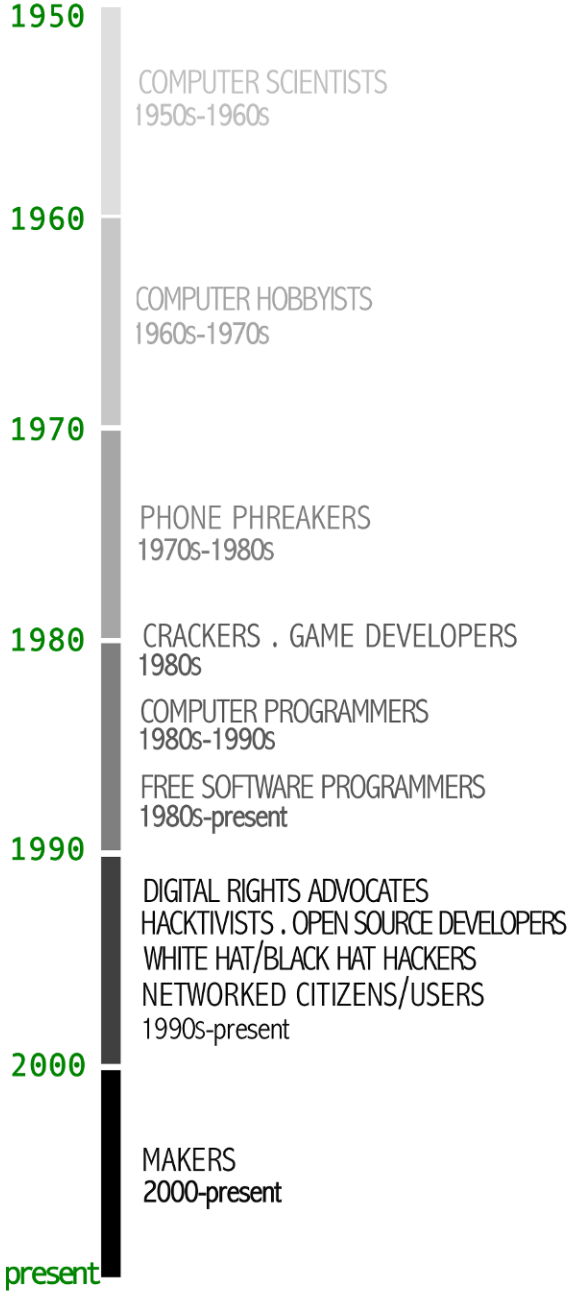
- Open versus closed
- Access over authority or being authorised
- Technical skills and solutions come first
- Freedom of speech and expression versus control
- Privacy not surveillance
- Self and/or community development

“Legal” crackdowns



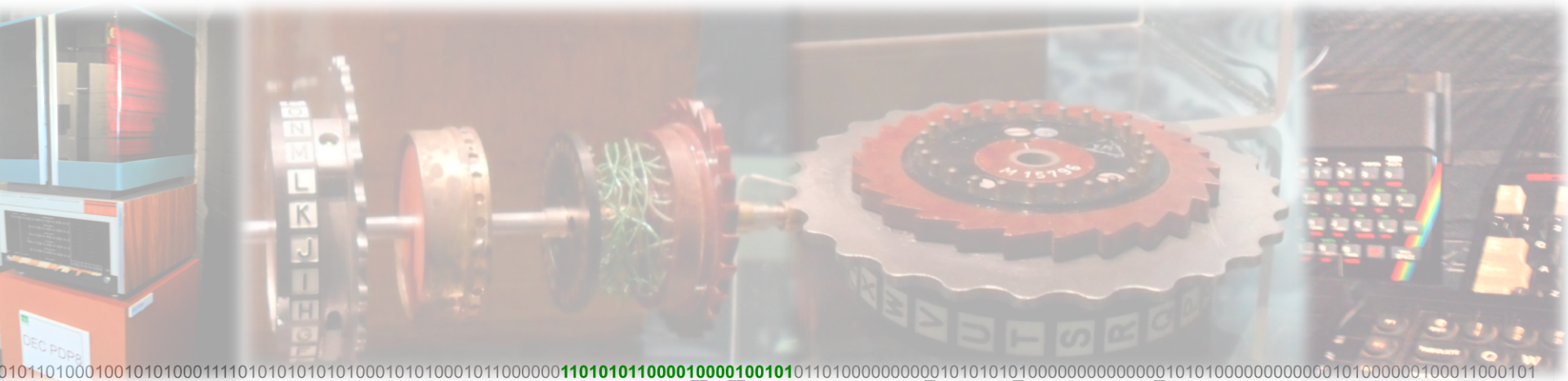
Criminalisation

- Criminalisation of hacking (1980s)
  - OECD report on Computer-Related Crime
  - US Computer Fraud and Abuse Act (CFAA) and UK Computer Misuse Act (CMA)
  - COE Convention on Cybercrime
- Law enforcement and prosecution
  - Few actual crackers prosecuted or convicted
  - Most cases involved disloyal and disgruntled employees

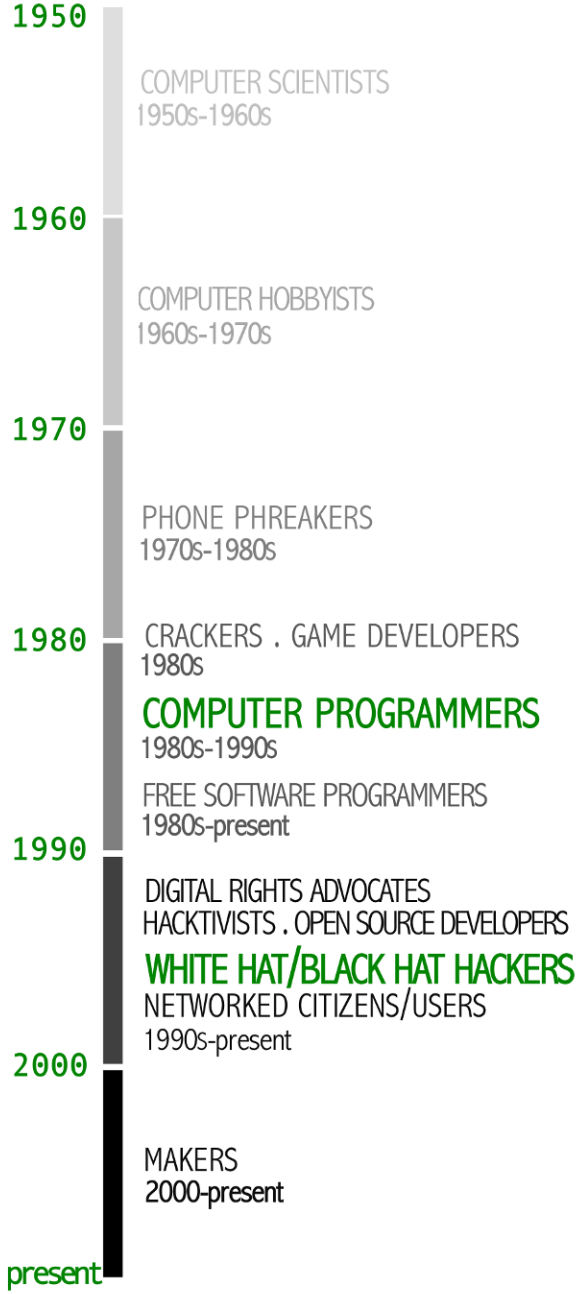


Legal restrictions

- Restrictions on access to and use of information and technologies
  - Confirmation of copyright and recognition patents over software (1980s)
  - Anti-circumvention provisions of the WIPO Internet Treaties (1996)

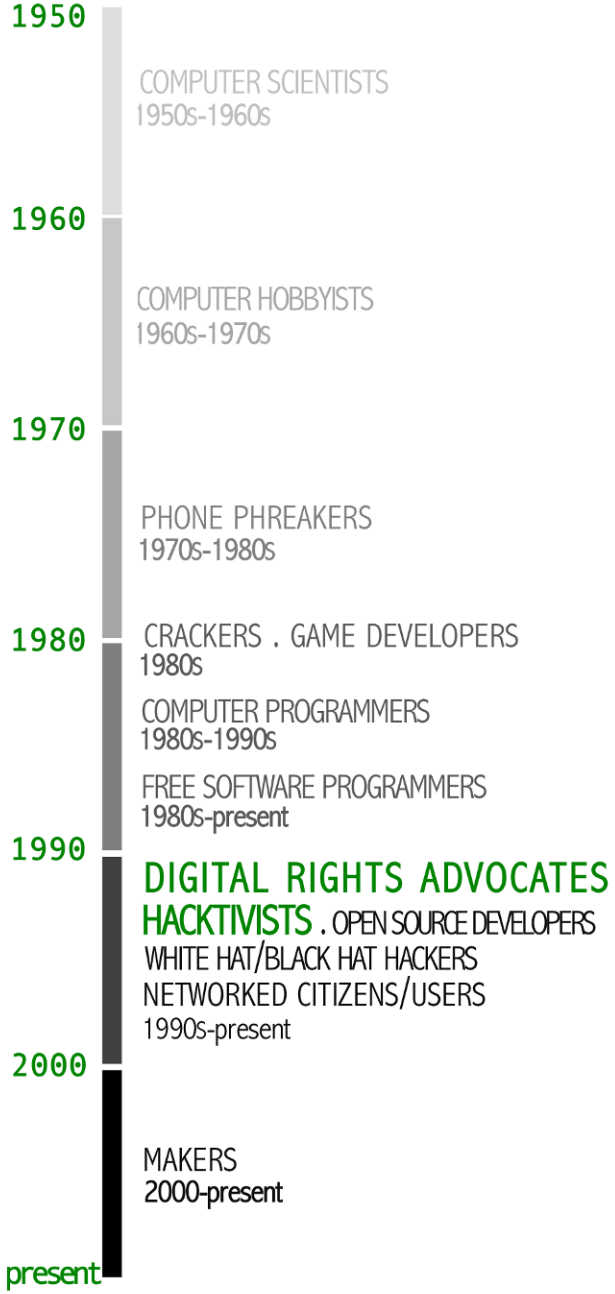


Mutual shaping of hacking & technology regulation



Technological workarounds

- Unintended consequence – greater and more creative forms of hacking
- Technological workarounds
  - Privacy-enhancing technologies and strong encryption (ex. PGP case)
  - Circumvention technologies (against DMCA)
  - Reverse engineering, interoperability and fair use (under IP law and relevant software laws)

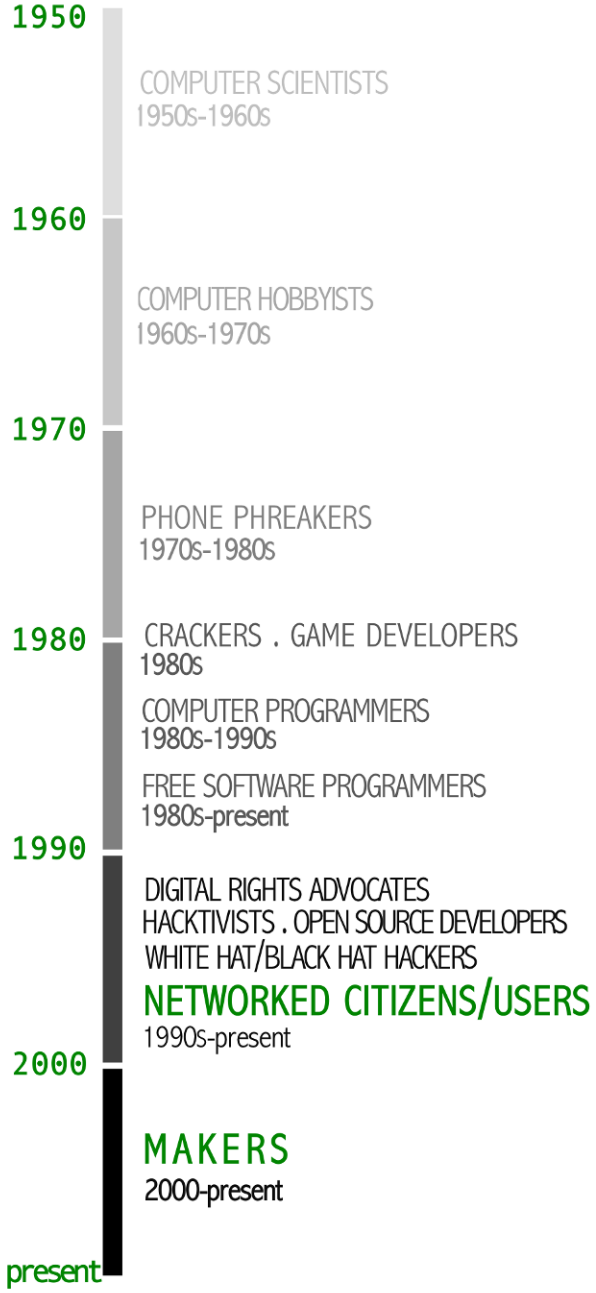


Politicisation of hackers

- Politicisation and self-organisation
- Emergence of digital rights advocates and hacktivists
- Involvement in legislative processes and judicial proceedings (ex. software patents in Europe, US SOPA and net neutrality in Netherlands)
- Resort to radical social action and protest (ex. Sony vs GeoHot)

Hacker norms as law

- Creative subversion of state law by non-state law
- Free and open source software (FOSS) and its licences guarantee four software freedoms
  - Freedom to run
  - Freedom to access, study and change
  - Freedom to redistribute
  - Freedom to distribute modified versions



Rights & freedoms of users

- Internet access as a human right and bill of internet rights
- Makers' Bill of Rights – technology must be
  - Easy to open and access and have instructions available
  - User serviceable and modifiable
  - Interoperable and have standardised and replaceable parts

1950

COMPUTER SCIENTISTS
1950s-1960s

1960

COMPUTER HOBBYISTS
1960s-1970s

1970

PHONE PHREAKERS
1970s-1980s

1980

CRACKERS . GAME DEVELOPERS
1980s

COMPUTER PROGRAMMERS
1980s-1990s

FREE SOFTWARE PROGRAMMERS
1980s-present

1990

DIGITAL RIGHTS ADVOCATES
HACKTIVISTS . OPEN SOURCE DEVELOPERS
WHITE HAT/BLACK HAT HACKERS
NETWORKED CITIZENS/USERS
1990s-present

2000

MAKERS
2000-present

present

Hacking is normative

Michael Dizon

http://michaeldizon.wordpress.com/

https://plus.google.com/112257762857266088814/posts