Chaos Computer Club

Submission
Global Digital Compact

Elina Eickstädt, Constanze Kurz

27 April 2023

Preliminary remarks

The Chaos Computer Club (CCC) is the largest European hacker association and has worked on issues relating to technology and its impact on society for over forty years. Since the beginning of its existence, the CCC has recognized and propagated the opportunities and possibilities that digitization holds. Questions regarding communication, data protection, data retention, surveillance, hacking, voting computer, freedom of information, copyright and computer art have been at the heart of CCC's efforts.

This submissions is a compilation of demands and recommendations the CCC made with regards to the key topics of human rights online and data protection. As a hacker association CCC's main focus is on the technical aspects and implications of regulations.

The intransparent and overlaying bureaucracy of the process of the GDC shows all the indicators of missing participatory internet regulation processes we've seen in the past on national and EU level. The negotiation of the

Data Protection

Protection through encryption

Human rights activists, journalists or opposition members can leverage secure technical procedures to protect themselves and their sources. In many countries, these groups or individuals operate at great personal risk. It is therefore important for them to be able to communicate unobserved using secure tools.

Encryption is fundamental for secure communication. It is essential that encryption methods are neither weakened nor undermined with backdoors.

The protection of human rights worldwide is increasingly becoming a question of technology policy. People who are affected by or report on human rights violations are imperatively dependent on technical means to secure their work. All efforts in democratic states to restrict or puncture technical means of encrypting communications and information for the purposes of law enforcement and intelligence services lead directly to a drastic deterioration of the situation for these individuals in their countries.

Biometric surveillance

The most important customers for biometric systems like facial recognition systems, speech recognition, iris or fingerprint scanners are government institutions, followed by airports. In these two areas, more and more money is spent each year on the acquisition and maintenance of biometric surveillance systems worldwide. In addition, biometric surveillance is no longer used or planned on a selective basis, but on a large scale, and government agencies regularly store the biometric data.

Biometric technologies are error-prone but have shown considerable progress in the last decade and thus become a threat to passers-by recedes into the background. The face in particular is typically exposed, so that optical scanning and recognition of biometric images can be carried out unnoticed. Errors that lead to spurious hits in many biometric software products are often discriminatory against certain groups of people and have inherent biases.[5]

Facial recognition as a screening measure threatens human rights and discriminates against groups of people, especially when it is automated. It is now one of the greatest threats to human rights and political participation. Therefore, we call on a ban on automated facial recognition in public, in particular its use by state actors.

[5] Cf. NIST: Face Recognition Vendor Test.
https://www.nist.gov/programs-projects/face-recognition-vendor-test-frvt

Analysis of digital lifes

The technological trend is toward integrated surveillance that link data from all systems where digital traces of life is collected. People are tracked by their digital shadows, for example via data from payment transactions, public transport tickets, cell phone data, surveillance cameras with automatic facial recognition and by mining social media data streams. All these and other data sources are integrated and analyzed with data analytics software and also machine learning software.

Systems suitable for implementing such holistic monitoring with multiple data sources analyzing mundane digital life traces of people should be banned. Funding priorities should be shifted to focus on technologies that protect against surveillance.