1. Welcome to this brief, 10-minute overview of digital privacy as recognised by the European Court of Human Rights.

2. In this time, I shall cover digital privacy as a human right, the two main sections of the European Convention on Human Rights under which violations occur, and touch on decisions that the Court has reached.

3. The Convention is an international treaty between 47 Member States that seeks to protect certain rights of individuals from State violation or interference. The Court upholds the treaty by determining whether a violation has occurred.

State authorities, and not companies themselves, are subject to the Convention, but States will be regulated for encouraging or allowing violations (by companies) within their own legislation.

4. Referring to “digital privacy” as a human right covers a broad range of activities. This includes communication with others, sharing or accessing information, publishing or expressing an opinion online, and the surveillance of online activity.

These different facets of activity can be traced, monitored and collated into profiles, to then be used by State entities or private companies for varying purposes including monetary or political gain.

With this in mind, there are two main sections of the Convention that are referred to when considering human rights violations relating to digital privacy: Article 8 and Article 10.

5. Article 8 concerns the right to private life and correspondence. Online activities could include communication with family and friends, exploring political beliefs or sexual orientation – activities many would prefer to not have documented about them. On the extreme end, Article 8 protects correspondence between a whistle-blower and news outlet, or human rights lawyer and client.

It is important to note that Article 8 is a qualified right, meaning a State may violate these rights in some circumstances. The State must establish that there is a legal basis for the interference, and that their actions are necessary for a democratic society in order to pursue an interest such as preventing crime or national security.

6. Article 10 concerns the freedom of expression. Online activities include publishing an opinion online, and sharing or accessing information and websites. It also seeks to protect people like journalists or human rights activists, who may otherwise be censored and imprisoned by the State for expressing their views.

Article 10 is also a qualified right, resulting in many court battles between publishing companies and Member States.

7. There are two main cases before the Court concerning digital privacy and State surveillance. Both received initial rulings, and will be considered further on the question of whether State surveillance programs are, in principle, a violation of Convention rights.

The first case, *Big Brother Watch v. UK*, was launched by a group of human rights charities against the UK as a result of the Snowdon revelations, concerning the bulk retention of communications data. The Court ruled that there were breaches of both Articles 8 and 10 – particularly regarding the lack of quality oversight of the program, and interception of correspondence between journalists and their sources. The Court did not consider the program itself to violate Convention rights.

The second case is *Centrüm för Rättvisa v. Sweden.* It was also launched by a human rights organisation that challenges State interferences, on the basis that their communications were at risk of interception by State intelligence agencies.

Although being at risk of interception can amount to an interference [95], the Court ruled that there was no Article 8 violation as Sweden's bulk communications retention was reasonable in the interest of preventing crime and terrorism.

8. We have heard today about the asocial nature of social media, and you may be wondering where companies such as Facebook fit into the scheme of European human rights.

Max Schrems, an Austrian privacy activist and lawyer, together with his company NOYB, has launched a number of cases against social media giants using the General Data Protection Regulation, most notably against Facebook Ireland.

The GDPR is a way of regulating how personal data is held and shared, and extends to cover any organisation that collects or processes such data.

In December 2019, a preliminary ruling in the Court of Justice of the European Union was published concerning Facebook's transfer of personal data to the United States under the EU-US Privacy Shield, where the data would be subject to interference from US intelligence agencies.

The Advocate General's opinion weighed the need for reasonable pragmatism to allow interaction with other parts of the world against fundamental values, specifically privacy rights, enshrined in EU legal orders including the Convention.

(Beginning [251]) He concluded that the transfer to the US of Facebook data, where intelligence agencies would have access to both content and metadata for their own use, amounts to an interference of Article 8 rights [256], without adequate legal protections [271], [308], and thus would fail to meet the criteria set out in subsection 2 of Article 8.

This case is on-going, and will be watched by many privacy enthusiasts with interest.

9. Finally, the Cryptoparty works to provide tools, tactics and guidance to gain control over the flow of your information, some of which will be demonstrated in the next talk.

Here are some examples of how the techniques and software choices tie in to the human rights interferences we have discussed.

To protect communication, encrypted services can be used.

Information access can be improved through choices of browser and search engine, deleting or preventing cookies, and a discerning use of social media.

Generalised State surveillance of online activity can be mitigated by obscuring internet connections through using the TOR project, a Virtual Private Network or alternative Domain Name Service.

Although a lot to take in all at once, these tools hold especial value for those who wish to challenge State activity and human rights abuses in safety, as well as those who just wish to keep their private life, private.

This brings us to the next talk, where more information on practical tools will be provided.

Thank you for your attention.