Motivation

The digital world from its very inception has not been even in all its parts: some issues have been relatively neglected and have not kept up with rapid technical and market changes. Among these are questions relating to digital identity, data security, and consumer privacy. This lecture examines the rapidly changing technological and social environment surrounding the individual and the blurring boundaries between the public and private spheres of existence.

4.1 – The digital individual

4.1.1 – From person to personae

Users of digital technologies today have a wide scope for constructing their identity. The mostly nameless and faceless environments of cyberspace create an ideal background for developing alternate identities or digital personae. The Internet makes it fairly easy for individuals to create multiple representations of their identities, depending on the context and exchanges involved. The phenomenon of online avatar has served to make these more popular and accepted: an avatar is an icon or representation of a user in a shared virtual reality space.

4.1.2 – Blurring boundaries and digital interactions

An individual in today's world spends more and more time using digital means to communicate. As such, many aspects of daily life are increasingly mediated by technology and this has important implications for human interaction and social behavior. The growing use of mobile phones has been blurring the boundaries between the private and public spheres of existence. Mobile phones have transformed the way people interact: revealing yourself when phoning has become expected.

Wireless e-mail and SMS have created another related phenomenon, that of the "permeability" of the separate contexts of social life. People are frequently interacting with others present in their physical space and simultaneously messaging with other "remote present" persons. This form of intrusion in any given social context has become commonplace.

Thus, it would seem that a sufficient connection between online and offline identity is required for societal purposes.

4.2 – Virtually private

The advent of the digital world implies a progressively ambient use of technology and communications. This in turn leads to an increase in the amount, quality and accuracy of data generated and collected.

4.2.1 – The value of privacy

Privacy: the quality of state of being apart from the company or isolation, seclusion or freedom from unauthorized oversight or observations; a place of seclusion or retreat. Over the ages, privacy as a concept was not explored in much detail, and was not a popular subject of consideration. Today, monitoring by all sorts of agencies seems to have become regular practice. It might be rightly argued that digital technology has not been developed for the purpose of invading privacy. But today, with the wide and almost universal means of data acquisition, this is less and less the case.

4.2.2 – Privacy and digital ubiquity

The vision of digital ubiquity (the state of being everywhere at once (or seeming to be everywhere at once)) is based on long-term vision of the increase in the power of microprocessors, and also seems applicable to other parameters such as storage capacity and bandwidth. As digital innovation gathers even more speed and as the information environment becomes pervasive and intensely functional, tracking and monitoring will become commonplace. Data collection would cross not only the boundaries of space, but also of time. Data about an individual or a group in a digital environment can be used for beneficial as well as nefarious purposes.

4.2.3 – A delicate balance

The gathering, processing and analysis of information are crucial aspects of today's digital information economy. There is a balance to be struck, however, between the need to harness the power of information for economic progress, quality of life and convenience, and the need to curb potential abuses relation to its collection and distribution. Many states have made attempts to manage data pertaining to their citizens and the European Union attempted to harmonize its data protection legislation across its member states.

4.2.4 – Current solutions for enhancing privacy

Though much has been done since the 1970's for developing legal principles and provisions for the protection of privacy. This has led to the growth of a number of so called privacy-enhancing technologies (PETs) with the aim of giving users greater control over their personal data. These can be thought of as falling into three categories:

- **Proxy**: it prevents the receiver of a message from identifying a sender.
- **Informed consent**: protecting privacy through informed consent includes the popular Platform for Privacy Preferences (P3P). P3P is an open standard that a given website can use to describe how it uses personal data collected during any session.
- **Untraceability**: protecting privacy through the absence of traceability.

In addition to the PETs, improvements in cryptography have been contributing to the growing security of data. Cryptography does not ensure the absolute protection of privacy, but the denial of it to unauthorized parties. A popular example is PGP, SSL and TSL. There are two forms of cryptography: symmetric (private key cryptography) and asymmetric (public key cryptography).

Tools for enhancing privacy should be made part and parcel of the digital world, and not just a ragtag assortment of software left to the user to use or not use.

4.3 – Managing identity in a digital world

The notion of identity is complex. It incorporates not only philosophical considerations but also legal and practical ones. Identity is what makes individuals the same today as there were yesterday (**sameness**), but it is also what makes them different from one another (**uniqueness**). Underlying identity is the distinction between the private and the public spheres of human existence, and as such identity and privacy are forcibly linked.

4.3.1 – The changing nature of identity

Identity:

- **Sameness** of essential or generic character in different instances, in all that constitutes the objective reality of a thing and the condition of being the same with something described or asserted.
- **Individuality**, the distinguishing character or personality of an individual, the relation established by psychological identification.

In the past, geography, community and family relationships defined human identity. In today's world, the individual has even more choices, covering more aspects of life. Today, most people carry some form of identification on them at all times. In the past, the declaration of an individual's name was sufficient to prove their identity. This is no longer the case.

4.3.2 – Vulnerabilities and rationale

The Internet was developed without a coherent mechanism for determining to whom and to what a user might be connecting. Although most site require some form of identification or registration, many of these are fairly basic and do not communicate any form of centralized registration system on other sites. Users are often obliged to form or select usernames and passwords that are mnemonically difficult to remember, this has led to an every-increasing burden of usernames and passwords for the user to carry, each associated with different websites. Many users feel obliged to resort to unsafe practices, like using the same password for different services. This may cause security breaches and leave them vulnerable to the machinations of identity thieves.

Identity management systems can empower users to regulate their activities online, and serve to install trust in information networks that are seen to be increasingly vulnerable to misuse and attack. For businesses, identity management can confer a number of benefits, for instance, reduce the complexity of multiple users managing, entering and using their premises. This would also facilitate the management of changing roles of users in the organization.

Important limitations are that today's systems are insufficiently equipped to deal with the rising number of interactions occurring in the digital space. Another source of concern is that the current network infrastructure suffers from security problems, due to persistent difficulties, with viruses, worms and spywares. Serious information leaks have been known to occur, compromising entire data systems.

4.3.3 – Designing for trust and predictability

Digital identity refers to the online representation of identity. More specifically, it refers to the set of claims made about a user or another digital subject. A claim is an assertion of the truth of something, typically one that is disputed or in doubt. Digital claims can be made up of sets of data, also known as attributes or identifiers. Attributes can include a name, a date of birth, currency used, preferred language, etc. Attributes also ensure that the distinction between the public and private spheres of individual lives remains intact. In order to establish trust between parties in the digital world, a subset of digital identity attributes needs to be communicated. The context will determine which subset of attributes is required.

The process of digital identity management consists of three main phases:

- **Verification** refers to the mechanisms which establish or create an identity, and which can later be used to make claims.
- **Authentification** is the process of establishing trust in a claimed identity.
- **Revocation** is the process of rescinding an identity an individual has been granted.

Digital identity management includes a number of different technologies that administer verification, authentification and revocation.

The European Commission's approach to the question of illicit interactions and identity theft was first expounded in its **PRIME** (Privacy and Identity Management for Europe) project. The objective of the project is to five individuals sovereignty over their personal date and to enable individuals to negotiate with service providers the disclosure of personal data and conditions defined by their preferences and privacy policy.

One of the newest trends in digital identity management is the federated system. A federated identity system is one in which no single entity operates the system, and one which creates an environment in which users can log on through a central identity provider and use the state of being authentificated to access resources across numerous domains. Federated systems go a step beyond simple single sign-on (SSO) systems. Where SO relied on setting up a central server to be accessed by each application, the notion of federation implies that local applications can respond to both local and remote queries.

4.3.4 – The road ahead

Through the importance of digital identity mechanisms is finally being recognized, much work remains to be done. Information regarding individual identities is becoming an increasingly valuable commodity, and as a consequence, its protection and management has become a pressing matter. In this regard, global standardization efforts and open source initiatives are crucial.