IDENTITY

Identity is a highly complex nexus of conceptions with numerous implications for privacy. Broadly speaking, such conceptions can be sorted into three groups – the metaphysical, the other-directed, and the other-generated.

A metaphysical idea of identity related to essential matters pertaining to an individual. That which distinguishes the individual from everything else is its identity, the relation that it bears only to itself, otherwise called *numerical identity*. This often persists through time, creating philosophical problems about how numerical identity is established (how do we know that this person is the same person as the child in this photograph taken 50 years ago?). A human individual's numerical identity over time is often referred to as their *personal identity*. There are many deep questions as to whether personal identity resides in a self or soul, or spatiotemporal continuity of the body or mind, and there are many paradoxes which may be illustrated with science fiction counterfactuals.

An other-directed idea of identity aims to present an individual to others in a certain way. This may help the other to distinguish the individual – for example, certain physical characteristics are helpful for this purpose, such as the face, as are labels such as the name. Such conceptions may also help individuals to assimilate into social groups, as when a person identifies as a particular gender, nationality or religion. One can have a cultural, political (in a class, or a party), national, sexual, racial or ethnic, professional, or generational identity, among others. Such identities are often signalled by individuals in the ways they speak, dress or present themselves.

An other-generated idea of identity is created by a nation, civic society, group, institution or computer system in order for it to be able to distinguish and single out those individuals it deals with. Such identities typically generate identifiers or credentials, including passports, ID cards, social security numbers and other labels, non-obvious biometrics such as fingerprints, behaviours such as purchase histories, associations with devices signalled by cookies, and passwords, all of which serve to confirm that the individual is indeed the correct individual from the point of view of the institution. When another gains access to such an identifier, they can present themselves falsely as the original individual, a process known as *identity theft*.

Identity affects privacy in many ways, principally as the means of singling out an individual and providing a route of access to that individual from others. Furthermore, if two identifiers can be linked to the same identity, an individual can be traced across systems. The absence of such a means entails that the identity of the individual is concealed, resulting in the individual being *anonymous*. Other-generated identities are a particular issue, as individuals may not have much input to or control over the means used to distinguish them – a point which may be seen as an assault on their human dignity. To address this latter problem, the idea of *self-sovereign identity* has emerged, where individuals manage computational resources to generate their own unique identifiers which will suffice to identify them to others.

Relatively little has been written on what constitutes an 'identity' in the context of digital information. Mourby and Mackey have argued that the benchmark for when information can be considered an 'identity' lies in its capacity to impact an individual. Rather than suggesting that privacy is engaged when an individual is identified, they suggest that 'identity' should be understood when some aspect of privacy—intrusion, monitoring, profiling, reputation, or autonomy etc. — is likely to be affected by the information. As such, identity in information (and thus identified data) lies in the capacity to engage the values and interests captured by the idea of 'privacy.'

Further reading: Kerr, I., Steeves, V. and Lucock, C., eds., 2009. *Lessons from the identity trail: anonymity, privacy and identity in a networked society*. New York: Oxford University Press.

Martin, R. and Barresi, J., eds., 2003. *Personal identity*. Malden, MA: Blackwell.

Martin, R. and Barresi, J., 2006. *The rise and fall of soul and self: an intellectual history of personal identity*. New York: Columbia University Press.

Mourby, M and Mackey, E. 2023. Pseudonyms, Profiles and Identity in the Digital Environment. *In*: van der Sloot, B. and van Schendel, S. eds. *the boundaries of data: technical, practical and regulatory perspectives*, Amsterdam: Amsterdam University Press, [**pages forthcoming**].

Sullivan, C., 2018. Digital identity – from emergent legal concept to new reality. *Computer Law and Security Review*, 34(4), 723-731, https://doi.org/10.1016/j.clsr.2018.05.015.

See: SELF, IDENTITY ASSURANCE, IDENTITY DISCLOSURE, IDENTITY MANAGEMENT, ANONYMITY, ANONYMISATION, IDENTITY THEFT, SELF-SOVEREIGN IDENTITY

PRIVACY

Privacy is a concept that covers an enormous range of connected and disparate phenomena, as this dictionary attests. Lexicographical dictionaries emphasise withdrawal of or lack of access to a private person or matter, freedom from attention, and seclusion.

The difficulty in making such a complex idea pragmatically usable was cited by Daniel Solove, who argued that 'privacy' was really a family resemblance term, a arguwith different uses of the term having various things in common between them, but nothing common to all of them. Kieron O'Hara, whilst endorsing this position, argues standard usage of the English term 'privacy' typically covers a range of ideas: informational privacy, decisional privacy, private property, psychological privacy, ideological privacy, spatial privacy, attentional privacy and extrinsic privacy (or obtrusion). Each of these exhibits aspects of the lexicographical definition, while their range testifies to the abstraction and fluidity of privacy.The idea of privacy is fluid across time and context, and can be significantly shaped by social movements and technological development. For example, the idea of 'bodily privacy' took on a particular significance in North America following second-wave feminism and *Roe v Wade.* More recently, while common understanding of the 'private' sphere has arguably been altered since the world wide web permeated our domestic lives.

Further reading:

Nissenbaum, H., 2004. Privacy as Contextual Integrity. *Washington Law Review*, 79, 119.

O'Hara, K., in press. *The seven veils of privacy: how our debates about privacy conceal its nature*. Manchester: Manchester University Press.

Solove, D.J., 2008. *Understanding privacy*. Cambridge, MA: M.I.T. Press.

See: ATTENTIONAL PRIVACY, BODILY PRIVACY, CONTEXTUAL INTEGRITY, DECISIONAL PRIVACY, IDEOLOGICAL PRIVACY, INFORMATIONAL PRIVACY, OBTRUSION, PRIVATE PROPERTY, PSYCHOLOGICAL PRIVACY, SPATIAL PRIVACY

SECURITY

Security is the protection against or reduction of vulnerabilities to external harm. Many protective security systems function to protect privacy either directly or indirectly. *Information security* involves holding information in such a way that unauthorised people cannot gain access to it, while *cybersecurity* is a similar concept applied to computer systems. *Secure communications* cannot be intercepted by eavesdroppers. *Home security* and *corporate security* describe systems for protecting private property.

Further reading:

Anderson, R., 2020. *Security engineering: a guide to building dependable distributed systems*. 3rd edition. Indianapolis: John Wiley.

See: SECURITY ENGINEERING, SECURITY BY DESIGN, SECURITY INFORMATION MANAGEMENT, INFORMATION SECURITY

TRUST

Trust is confidence that another person (or system) is *trustworthy*. In property law, someone who trusts is a *trustor*, and a trusted person/system is a *trustee*. If someone is trustworthy, they must have the capabilities, willingness, and incentives to act in the interests of the trustor. A trustworthy person will tend to meet their commitments to trustors, while a trustworthy system can be relied upon to meet its specification.

The problem of trust is how, under conditions of uncertainty where future behaviour of the trustee can only be estimated, to ensure that all and only trustworthy people/systems are trusted. A trustee is usually trusted in some limited domain (for instance, trusted to supervise children but not trusted with administrative tasks). *Placing trust* in a trustee involves the trustor taking a risk, because they will rely on the trustee fulfilling their commitments.

An *untrustworthy* person is either unable, unwilling, or not incentivised to act in a trustor's interests. A would-be trustor *mistrusts* or *distrusts* a person/system if they believe that the person/system is untrustworthy. Mistrust/distrust are therefore not simply the absence of trust, but a positive judgment of untrustworthiness.

The failure of a trusted person to deliver their commitments is usually seen as fatal to trust. On a common model, trust is built up slowly as the trustee provides evidence of their trustworthiness to the trustor but can disappear immediately if the trustee fails. Empirically, this is not always the case, but security engineering assumes that failure to deliver security commitments is catastrophic.

Privacy and trust are often linked in the computing literature. Data subjects are seen as trusting others with their personal data – in other words, believing that the data controller is able, willing and incentivised to hold their data securely. The discipline of *trusted systems engineering* is rather misnamed since it is actually aimed at engineering trustworthy systems. It cannot be guaranteed that they will be trusted, since this depends on the external perspective of the trustor, not on the engineer's work.

Further reading: Hawley, K., 2019. *How to be trustworthy*. Oxford: Oxford University Press.

O'Hara, K., 2004. *Trust: from Socrates to spin*. Duxford: Icon Books.

See: SECURITY, FAIR INFORMATION PRACTICE, INFORMATION ETHICS, DATA GOVERNANCE, RISK, DATA SUBJECT, DATA CONTROLLER