Juliet Lodge:

The promise of ethical secrecy: can curiosity overcome automated group-think?

Abstract:

Secrecy and transparency are fundamentally undermined by automated decisionmaking that transforms our understanding of where we begin and end, of self and society. This article considers whether and how technological applications compromise secrecy, transform our perception of the idea appropriate disclosure, our interaction in society and the society itself. It argues that secrecy is part of a continuum of transparency and accountability that cannot be reliably sustained and mediated by automated decisionmaking devoid of curiosity. Do we need an ethics of secrecy derived, perhaps, from our understanding of harmful effects of disclosure?

Agenda

Author:

Prof. Dr. Dr Juliet Lodge

- Jean Monnet European Centre of Excellence, University of Leeds, LS2 9JT,UK.
- ✉ j.e.lodge@leeds.ac.uk

- Relevant publications:
  - (2011) ‘Transformative biometrics and the exercise of arbitrary power’, in A.Bromme, C.Busch(Eds) Biosig. Fraunhofer Institute. Darmstadt, Gesellschaft fur Informatik.67-78.
  - (2010) Quantum Surveillance and shared secrets: a Biometric step too far? CEPS, Brussels, 2010
  - Biometrics in the EU, Report for the LIBE committee of the European Parliament, Brussels, 2010.

'We are neither a society of angels nor one of devils, neither a fully open society nor a secret one. This is the reason why the difference between public and private as well as between public and secret is so relevant for every human society'[1]

1 Where do I begin?

As every parent knows, part of a baby's development is about the exploration of the limits of the physical self. As a baby plays with his toes, he discovers limits: where do I begin and end? As he moves on to engage in and arguably depend on an ICT enabled world, the binary self-other distinction that provides content for conceptions of internal and external, private and public, subject and object becomes increasingly murky. Machines, even RFID - or nano therapeutic medical - implants, condition his behaviour, sometimes imperceptibly and without him consciously noting as much. Sometimes overtly, in denying or facilitating access to space, goods and services, as in the case of automated border controls.

This rather mundane example of denial of access, however, highlights a tension in our understanding of identity, how we identify ourselves in private and in public and how that is captured by machines that have the capacity to intrude on and dissolve the border between the self and other, the internal and external, the private and public. This gives rise to anxiety over personal space and privacy. It also leads to a disingenuous countervailing rhetoric on 'open government' which has little to do with transparency and accountability, and much to do with the processes that lend themselves to being depicted or enacted by computer code. Putting government or public authority information (such as civil registration documents, committee meetings, government structures and so on) online does not equate to openness. Pictograms and dates are useful and essential for *response, reflection and external input.* These merely suggest that such domestic civil procedures are not hidden: secrecy is not the dominant norm.

Contrast that with: personal online activity, whether in social media or accessing of services; corporate online behavioural tracking; malevolent intrusion, and e-crime. There, invisibility and in effect 'secrecy' to facilitate evasion from immediate detection for whatever reason, are common. Here the personal and the private become commodified and re-configurable (with or without the individual person's explicit knowledge or consent). In that case, something occurs 'in secret', possibly to their detriment and certainly in a way that in some measure exploits and capitalises on them. Is it possible to identify and define ethical secrecy?

1.1 Lies, damned lies and secrets

Secrecy has become a dirty word in politics. Secrecy is suspect. But it is not the antithesis of transparency. A more nuanced appreciation is necessary. Without curiosity, neither secrecy, openness, transparency and accountability are credible.

Secrecy is necessary to operational effectiveness in the administration of certain (normally extra-border, external) parts of public policy. Secrecy is intrinsic to our daily lives, not because we have something (shameful) to conceal but because we have something we choose not to reveal, or see as inappropriate to disclose in specific situations. This neither makes us suspect nor does it mean that secrecy and transparency are not part of a continuum of private and public life. Appropriate disclosure helps ensure civility. If everything is potentially open to being disclosed, with or without the subject's knowledge let alone informed consent, is secrecy robbed of meaning? How is our world and society transformed? Are there some conditions under which silence should imply not consent (as in the Anglo-saxon world) but intentional secrecy? Do we need an ethics of secrecy derived, perhaps, from our understanding of harmful effects of disclosure? The ethics of secrecy requires us to consider under what conditions secrecy has been justified.

[1] Capurro, Never enter your real data. 75.

1.2 Secrecy as a justifying rationale

Secrecy is a term traditionally associated with ensuring security. In western, liberal democratic tradition, secrecy has been put forward as the legitimate and justifiable exception to the rule of openness and transparency in order to safeguard a state's security and liberty. Security and liberty are part of the same continuum. However, the state's ability to sustain and enforce secrecy in the name of security and liberty has been eroded by many factors, including:

- technological innovation and new applications especially for mobile telephony
- robotisation and automation of processes previously requiring a human to exercise judgement and make an informed decision on the next step through the use of 'smart borders', RFIDs, nano-sensors, robots, ambient intelligent environments
- multi-use technologies, such as brain imaging and therapeutic interventions, for 'security' purposes
- public private partnerships and semi-privatisation in administering public government services (including aspects of security and policing)
- out-sourcing data and information storage, destruction and analysis beyond the borders of the state, including the cloud
- securitizing domestic politics (including leisure, education, health, civil document based data by requiring data retention for 'security' purposes)
- allowing data provided for one purpose to be re-used or reconfigured for imprecise purposes by unknown 'others' in the name of transparency broadly conceived and in order to maximize the value of open data
- automated cross-border information exchange[2]

Technological innovations and new applications have eroded the boundaries between the public and private world to the extent that their almost imperceptible, yet accelerating, merging makes it difficult to identify and relate to the traditional structures and norms of accountable actions. Critical infrastructure attacks, denial of service attacks, malware and intrusion can be conducted from outside the jurisdiction of the government or organisation that commissioned the programme running them. How, in such an instance, is government or the appropriate authority to be held to account? Legal liability to gain financial redress is too often paraded as the appropriate response when in practice it is merely a symbolic response. Claiming to exert control via ACTA, too, may prove chimerical by facilitating the very intrusive tracking by invisible machines/ISPs on private/secret activity that the ordinary person abhors. Informational self-determination is a laudable ideal, informed by ethical principles of tolerance, openness, purpose specification and informed consent. It is far from universally accessible, let alone – currently – operationally or technically absolutely possible.

The traditional idea of a visible face being linked to responsibility for performance is undermined by new technological applications. Who or what can we trust as reliable and under what circumstances is that trust warranted?

The same applies in the private realm. While some people lead imaginary second lives as fantasy avatars, others transform their cyber criminal exploits into tangible actions traceable and apprehendable by cyber police. The anonymous avatar is not technically synonymous always with a 'secret life'.

Identities and means of proving and claiming an identity that we thought we could rely on and trust (such as birth certificate, civil registration documents and passports) are only as reliable as the enrolment procedures for ensuring the authenticity of the original. Fingerprinting babies at birth and deriving a biometric 'breeder identity document' from that is not foolproof[3]. Moreover, false or poor quality breeder documents can multiply problems for genuine individuals long into the future. Yet, those agencies, ICTs or codes that

[2] Lodge,73.

[3] http://www.europarl.europa.eu/news/en/headlines/content/20120413STO42897/html/MEPs-question-Commission-over-problems-with-biometric-passports

generate them remain largely invisible or at least able to blame errors on 'computer code' without, at present, the public being apprised of the relative reliability and trustworthiness of the ICTs used. Commercially sensitive or politically, security sensitive information (however that is defined) continue to rely on the legitimating rationale of secrecy. However, if this can and is increasingly breached, should everything be in the public domain with a free-for-all or should there be an ethics of secrecy or practice that is informed by ethical secrecy?

2 Openness the antidote to secrecy to reconnect governments with citizens

To some extent governments have recognised that in invoking 'secrecy' rationales to legitimate their securitization of domestic politics requires a counter-weight. Accordingly, the rhetoric of 'reconnecting' with citizens through ICTs has been used to counter the charge of excessive securitization of domestic politics and the private realm by public authorities. This has not been adequately demonstrated in the case of public-private partnerships.

Among the attractions of ICTs for governments has been the illusion they have offered of making government appear more transparent and less secretive to citizens by reconnecting rulers and the ruled through, for example, 'open government', e-voting, online petitions and blogs. ICTs offer the mirage of facilitating benevolent reconnection of citizens both with each other in an e-public sphere and with political contestation, without offering the democratic counterweight of protection against the abuse of power. Instead, technical fixes and data protection laws have been advocated. These include, baked in security by design to make data privacy a first principle rather than an after-thought in the design of systems and applications.

But the preoccupation with privacy, its commodification and privatization, risks compromising our understanding of secrecy and the situations in which secrecy is a precondition of operationally safeguarding security and liberty, and an imperative for sustaining visible, public democratic accountability of those who administer processes and control access to them.

Governments have ceased to be the single, authoritative locus of authority or enabler of access to public services and protector of citizens' and territorial security. In a modern hyper-connected world, access or use of e-services is not simply a matter of digital literacy. The well-known inhibitors such as age, physical or mental incapacity, digital illiteracy, or poverty are dwarfed by technical applications that allow invisible agents to intrude, to deny access to services, to censor, or to cyber-attack critical infrastructures as well as individual people. The cloak of invisibility around malevolent cyber-attacks exacerbates the vulnerability of all: governments, corporations, citizens.

Whom to trust to safeguard security then becomes an interesting question. More interesting still, perhaps, is the question of whether informational secrecy in the public domain is a threat to individual and collective security? Should it be kept purely for our most personal private lives, even though that is technically impossible?

Is privacy itself so technically suspect and emptied of meaning that it is irrelevant to individual security and secrecy? Is the protection of an individual's ICT enabled identity token a necessary aspect of protecting that person's safety and security, or collective safety and security? Should such identity tokens be secretised? By whom, under what circumstances? For how long? Should secrecy be commodified? Is it realistic to expect government to protect state and personal secrecy? If governments were able to do so, would public trust in the credibility of government authority be restored? Can ethical secrecy be sustained by traditional, liberal democratic government structures and practices or does technological innovation and particularly automated, cross-border information exchange, constrain, dissolve or facilitate it?

2.1 ICTs and sustainable democratic accountability

As public administration is externalized, outsourced or shared in private-public ICT partnerships, the political master is replaced by a commo-techno (commercial-technological motor) that eludes public control, except possibly through the purse. The managerialist approach to ICT 'good practice' relies on voluntary, ad hoc and imperfect compliance. A quick fix to claiming transparent accountability, it veils the semi-privatisation of political accountability and differential security in opaque terms not susceptible to public, external scrutiny.

Data Protection and privacy commissioners and laws cannot effect sufficient politico-legal control. They are necessary when people with official documents that authenticate them (something not universal yet) are trackable by computer code. They are insufficient for protecting and allowing the data subject to discover and revise data held about him, and for allowing consistent and coherent access to data for use in criminal investigation for those responsible for investigations. This is not just a matter of relative forensic capabilities, data retention practices and ICT legacy systems, contrary to what the recent EU Commission Communication (2012) suggests). The blurring of responsibilities regarding e-information means that both public and private authorities tend to gloss over problems of accountability, or contest responsibility and/or capacity to pay when facing big fines. A British public health trust raised ethical questions when the British Information Commissioner's Office levied the largest ever fine following the sale in internet auctions of some of its defunct hard drives containing sensitive personal data by the IT provider. The trust suggested that the fine was disproportionate to its duty to provide health care in times of recession[4]. Should there be a hierarchy of ethics to reflect the relative value attaching to differential privacy, secrecy and implementing practices in public-private partnerships. e-commodification of personal information in fuzzy e-space is insufficiently susceptible to visible, authoritative public regulation and accountability. For constitutionalists, the assumed bargain between the state and citizen, aggravated by legal uncertainty, will be broken no matter how ubiquitous 'surveillance' in its many guises. Security is no longer simply a matter of safeguarding territorial integrity. ICTs' ubiquitous impact on citizens' lives and geo-cyber attacks on critical infrastructures are not amenable to the traditional defences offered by international treaties. Electronic networks link public and private organisations in ways that so far escape effective technical and political oversight and control. Is a tragedy of the increasingly re-bordered domestic and internationalised cyber-spaces of the ICT commons is inevitable?

3 Inverting the secrecy bargain

Transparency and accountability are essential to prevent an abuse of power and vital to allowing parliament to hold government in check. In fields traditionally subject to the security exceptionalism associated with secrecy rules and intelligence, questions arise over an assumed proper balance between the requirements of liberty and of security. While perfect equilibrium is unrealistic, creeping exceptionalism undermines sustainable liberty. If legitimacy is challenged by the people or worse still by invisible cyber-attacks, what are the prospects for the democratic exercise and locus of justice, authority and power? In such a scenario, does secrecy endanger security?

Absolute openness and absolute secrecy? What are the disruptive consequences of secrecy? Of refusing to share information in formerly trusted groups? Does dishonesty become the shield against breaches of secrecy, so that no one is ever (quite) who they say they are? While absolute secrecy is neither possible nor desirable, an element of secrecy is necessary to trust. Moreover, the artificial duality of absolute secrecy versus absolute openness is misleading because it misses the point of the necessity of the intervening variable of curiosity.

[4] Information Commissioner's Office (ICO). In June 2012, Brighton and Sussex University Hospitals NHS Trust was issued with a Civil Monetary Penalty (CMP) of £325,000 following a serious breach of the Data Protection Act in 2010. The ICO was granted the power to issue CMPs in April 2010.

4 Conclusion: Curiosity: the intervening variable

Without curiosity, secrecy is arguably not necessary. Without curiosity accountability becomes no more than a mechanical action, a knee-jerk reaction. Without curiosity, the disclosure and non-disclosure of information lacks purpose : the right to know and the right to be forgotten are mired in an expectation that someone or something somewhere is sufficiently curious to want to know or to forget and erase.

What is problematic about secrecy and ICTs is the possibility that (non) disclosure may cease to depend on human decision; that they may not be conditioned by precautionary considerations of whether or not exceptional circumstances justify the release of information without prior consent in order to prevent harm. Disclosure is not only part of the discourse of secrecy versus openess but also of individual and collective harm versus an evaluation of less intrusive/more conditional considerations regarding when, how and to whom disclosure should be made or secrecy preserved.

Once this decision is automated and becomes a mechanistic reflex where judgement associated with curiosity and reflection are absent, the potential transformative impact on society is extensive. Machines, computer code or robots that automatically disclose or withhold information do not necessarily refer to explicit moral values before doing so: those of the original, invisible and unaccountable programmer(s) determine what technical process is enabled. It is easy then to reflect on the duties of machines vis-a-vis humans without first considering what level and scope of data sharing, disclosure of secrecy might be contingent or legitimate in given circumstances.

Since machines are able to select and make linkages between data fields, and 'learn from other machines', group think is inevitably entrenched in how we conduct our lives. Is that group think potentially more dangerous than that experienced in policymaking circles in history? By reconsidering secrecy, could scientific innovation help to restore confidence and trust in our ability to strive for the common good through an ethical use of ICTs?

It is disingenuous to suppose that it would be safe to rely on machine-led disclosure and secrecy. What are the implications of attacks on hyper-connectedness? Here we are not concerned with IPR, duties of care, legal and financial redress. We are concerned with the ethical impact on society, how humans conduct their lives, human self-understanding, ICT substitution for realtime human reasoning, the technisation of the self, techno-dependency, the implications of the erosion of stable interfaces between man and ICTs, and the evolving digital values to sustain civilised society. We are concerned with how ideas of sufficient privacy and sufficient secrecy are being reconfigured as anonymisation codes of practice implying the elaboration of a hierarchy of ethical secrecy.

References

Capurro, Rafael (2011): Never enter your real data, IRIE,vol 16, 74-8.

Council of the European Union (2011) Commission Services Communication to the Working Party on Data Protection and Exchange of Information, Consultation on reform of Data Retention Directive: emerging themes and next steps, Doc 18620/11, Brussels, 15 December.

Information Commissioner (ICO) (2012) NHS Trust fined £325,000 following data breach affecting thousands of patients and staff. Press release. http://www.ico.gov.uk/news/latest_news/2012/nhs-trust-fined-325000-following-data-breach-affecting-thousands-of-patients-and-staff-01062012.aspx.

Lodge, J (2009) Transparency and Accountability: from structuro-procedural transparency and institutional accountability to communicating (in)security in digi-space in (D.Bigo ed) Europe's 21st Century Challenge: Delivering Liberty and Security.Ashgate