Philos. Technol. (2016) 29:293–305
DOI 10.1007/s13347-016-0217-3

COMMENTARY

The Secret in the Information Society

Dennis Broeders[1]

Published online: 14 April 2016

Abstract Who can still keep a secret in a world in which everyone and everything are connected by technology aimed at charting and cross-referencing people, objects, movements, behaviour, relationships, tastes and preferences? The possibilities to keep a secret have come under severe pressure in the information age. That goes for the individual as well as the state. This development merits attention as secrecy is foundational for individual freedom as well as essential to the functioning of the state. Building on Simmel's work on secrecy, this paper argues that the individual's secrets should be saved from the ever-expanding digital transparency. The legitimate function of state secrecy in turn needs rescuing from a culture of secrecy and over-classification that has exploded in recent years. Contrary to popular expectation, the digital revolution adds another layer of secrecy that is increasingly hidden behind the facade of the 'big usable systems' we work and play with every day. Our dependence on information systems and their black-boxed algorithmic analytical core leads to a certain degree of Weberian (re) enchantment that may increase the disconnect between the system, user and object.

Keywords Secrecy · Georg Simmel · Information society · Surveillance · Transparency

This paper is an adaptation of the author's inaugural lecture, delivered on 30 October 2015, when he formally took up his professorship on the chair of Technology and Society at the Erasmus University Rotterdam. He is indebted to Willem Schinkel and Huub Dijstelbloem for valuable and much appreciated comments on earlier drafts and to Linnet Taylor for translating the original Dutch text. The orginal lecture called 'Het geheim in de informatiesamenleving' (Broeders 2015) can be downloaded here: http://www.wrr.nl/fileadmin/nl/Presentaties/Dennis_Broeders/Het_geheim_in_de_informatiesamenleving_Oratie_Dennis_Broeders_okt_2015.pdf

✉ Dennis Broeders
broeders@fsw.eur.nl

[1] Department of Public Administration and Sociology, Erasmus University Rotterdam, Rotterdam, The Netherlands

[2] Netherlands Scientific Council for Government Policy, The Hague, The Netherlands

1 The Secret as a Social Category

Dutch daily newspaper NRC Handelsblad on 20 June 2015 carried an article titled 'Transparent citizens'. It was one in a series of articles that attempted to address significant current political problems. In this case, it was the question, 'who can still keep a secret?' This is a question that is extremely relevant in today's digital society. How can a secret be kept in a world where everything and everyone is connected by technology designed to map and to link together people, objects, movements, relationships, tastes and preferences? It is also an interesting issue given the social character of secrets. One cannot keep a secret by one's self. More than that, at the individual level, the difference between public and private is effectively meaningless. Strangely, secrets are social phenomena. Robinson Crusoe, when he thought he was alone on his island, had no need for secrets or privacy.[1] To keep a secret from yourself is—if possible at all—more a subject for psychology than sociology.

The social aspects of secrets are a well-established theme in sociology that in a theoretical sense is mainly linked to the work of the German sociologist Georg Simmel. A great name in classical sociology, who in most assessments stands amongst the greatest along with Marx, Weber and Durkheim. Simmel wrote at the start of the twentieth century of a 'sociology of secrets', looking at the function, the workings and the value of secrets for social life. The most important sociological meaning of secrecy was, according to him, external, since it creates a relation between the secret's owner and the other who does not know it.[2] Children create a social relationship when they say 'I know something you don't know'. If it were really supposed to remain secret, they would do better not to speak about it. A secret, then, has a value that is sometimes intrinsic, but may also often be external and social. Or as Simmel—a sociologist after all—would say, keeping a secret is a form of stratification. A secret is a possession that will also be coveted by others—he called the secret a jewel or an adornment—and, therefore, a symbol of the owner's importance.[3] I know something you don't know.

Simmel did not hide his appreciation for secrets when he called it 'one of man's greatest achievements'.[4] That appreciation has, I think, two facets. First, he believes that secrets make social life possible. Secrets are of fundamental importance for maintaining relationships. Or, as Craig puts it in his reading of Simmel, 'If I divulged every passing thought, I doubt I would keep my friends for very long: by keeping parts of myself secret, I maintain relationships.'[5] Anyone who tells nothing but the truth will soon find themselves very lonely. Above all, the fact that people have secrets, or better put, the fact that people are not fully knowable, is fundamental to the common trust that makes possible everyday interaction between people who do not know each other. For Simmel, that is a crucial element of modernity and urbanisation. In city life, people are simultaneously more individualistic and more dependent upon others whom they do not know.

Another element of modernity has to do with the changing arrangement between the state and its citizens, and with the role and legitimacy of secrets in that relationship. At

[1] Marx en Musschert (2009: 7)
[2] Simmel/Wolff (1950: 345)
[3] Simmel/Wolff (1950: 338)
[4] Simmel/Wolff (1950: 330)
[5] Craib (1997: 163)

the start of the twentieth century, Simmel saw a great shift with regard to secrecy on the meta-level of 'the state' and 'the individual'—both in quotation marks. In the nineteenth century, so much light was cast on matters of state that traditional secrecy—until then the norm for many state activities—was crumbling. At the same time, modern urban life gave the individual more opportunity than before to become hidden amongst the masses and to disappear. Simmel describes this dual development as follows:

> Politics, administration and jurisdiction thus have lost their secrecy and inaccessibility in the same measure in which the individual has gained the possibility of ever more complete withdrawal, and in the same measure in which modern life has developed, in the midst of metropolitan crowdedness, a technique for making and keeping private matters secret, such as earlier could be attained only by means of spatial isolation.[6]

In other words, the individual becomes free as she joins the masses. Through specialisation and division of labour in modern life, many relationships become more businesslike and impersonal. One can keep more private than before. 'Stadtluft macht frei' (the city air makes one free), one might say, although this mediaeval expression has a very specific historical and legal context.[7] Secrets are foundational to the bourgeois society, where the individual can shield himself and create a private domain that is no longer burdened with too much knowledge of the other. This allows for a private domain screened from the public gaze.[8] In this formulation by Simmel, the state has become more transparent. The Enlightenment brought the state's secrets into the light of day. At the same time, Simmel saw that the state was growing and diversifying and becoming less easily made accountable on an organisational level, which created more opportunities for secrecy.

Today's information society is an interesting case in terms of secrecy on the meta-level, both of the individual and the state. In 2015 it is harder for individuals to keep secrets and the government seems to have recovered its appetite for secrecy. Despite all the reports and well-meaning research on 'open government' and 'open data' the number of files, physical or virtual, marked 'secret' or 'classified' grows every day.[9] And it is at least a little worrying that government seems to permit the individual citizen ever-fewer secrets. With regard to citizens, the mantra of government is 'more information' rather than less. Information, even personal information, does not always equal a secret for everyone and at any time. Only when social tensions arise about information, it becomes about secrecy: I want to keep something secret that someone else wants to know. In the information society, secrets (in a sociological sense) are sometimes only revealed as such when information is made public. The social dynamic of revealing information means that some information is only retroactively realised to have been considered a secret. The ability to hide information—and the secrets therein comprised—is a form of freedom that requires others to keep a suitable distance, not in

[6] Simmel/Wolff (1950: 336–337)

[7] The expresion 'Stadtluft macht frei, nach Jahr und Tag' (city air makes free, after a year and a day) refers to a mediaeval principle of law that serfs who resided in a city for a year and a day were henceforth regarded free citizens of that city.

[8] Horn (2011: 112)

[9] See for example Curtin (2011)

the least the government. In the information society, my thesis holds, the individual's ability to keep secrets diminishes and the volume of state secrets rises, but those state secrets also become more vulnerable. Both developments are related to new technologies that themselves, in their turn, create a new layer of secrecy. Individual secrets, state secrets and the secrets of technology itself are central to this paper.

2 The State's Secrets

If secrets are important for individuals and for society itself, they are also important for states. Indeed, for states secrets may be a matter of life and death. There is a rich literature that discusses the role of secrets for states. Over the centuries state secrets have played various roles and have been driven and justified by different political logics. In an excellent overview, Eva Horn sets out the three most important forms of political secrecy.[10] And, in good academic tradition, they have Latin names. State secrets can be classed as *mysterium*, *arcanum* and *secretum*. These three terms not only denote a historical evolution but also explain how state secrets are viewed in a political sense. They highlight the role and legitimacy of state secrecy.

Mysterium comes from the middle ages and is a doctrine of political theology. It carries an implication of the unknown and the unknowable—the ineffability of God, the nature of the soul. The divine power of absolute monarchy has ineffable secrets that may not be disclosed, nor should be disclosed. *Arcanum* refers to the secret element of a more secular politic doctrine. The root of *arcanum* is *arca*, meaning chest or coffer. The secret, then, is something that is put away, hidden from the sight of the outside world that therefore knows nothing of it. Here, the secret is an instrument of power and of the retention of power, and thus more functional than moral or ethical, although the two are not mutually exclusive. The so-called *Arcana imperii* are doctrines of power with historical roots that stretch from the power politics of Roman emperors to the practices of some of today's authoritarian regimes.

Secretum highlights the social element of secrecy—as we saw on the level of society in Simmel's work. *Secretum* defines the secret in terms of social inclusion and exclusion. Where *arcanum* signified keeping information out of sight—so that in the social sense it simply is not there—*secretum* in contrast creates a relationship. A relationship between the known and the unknown, and above all, a relationship between those who do not know the secret and those who do, or who are presumed to know it.[11] In other words, 'I know something you don't know' also creates a social relationship on the state level, as much between different elements of the state apparatus as in the larger sense of the relationship between the state and its citizens. We live—as far as we know at least—in the era of *secretum*. There are many *known unknowns* that the state—in our name—keeps secret from us. We know that there are secrets, but we do not know their content. They know something we do not know. This social relationship between state and citizen is not without its tensions, when it comes to secrecy. In 2016 many citizens view

[10] Horn (2011), see also Quill (2014)
[11] Horn (2011: 107–110)

state secrecy with suspicion, which certainly has something to do with the expectations that modern democratic politics has created for itself. In the words of Eva Horn:

> A political culture that stresses transparency and moralizes the political cannot accept the constitutive role of the secret; it will, at best, treat it as a regrettable necessity.[12]

A democratic and moral politics has difficulty justifying the functional and instrumental use of secrecy. Anyone who follows the news is confronted with that on a daily basis. State secrets increasingly have an unpleasant flavour of the abuse of power and tend to be associated with corruption and the cover-up of mistakes. Revelations by journalists and whistleblowers such as Edward Snowden and Chelsea Manning confirm the public's suspicion that the state has 'dirty little' and 'dirty big' secrets. Certainly against a background of moralistic politics, with the demand for clean hands and the public profession of norms of open and transparent government, state secrets are increasingly viewed with suspicion.

So at first glance, it seems the state does not really want to keep fewer secrets. Certainly, many kinds of information that were previously treated as pivotal for the power of the ruler are now in the public domain. Philosopher Ian Hacking describes how the first censuses and statistics were classified as state secrets and anxiously protected because that information stood for power.[13] Today, national statistics agencies publish figures daily to show the state of the country. But over other issues the curtains have been drawn: many more documents and activities are seen as confidential or secret. And at the same, all kinds of government agencies collect ever more information about citizens. For all government roles, ranging from welfare provision to surveillance and control.[14] The enthusiasm of government for gathering, sharing and cross-referencing more and more data about its own people is only increasing with the advent of new technologies.[15]

3 The Fight for Secrets Is the Fight for Freedom

Here, we come to another important aspect of secrecy. Secrets are also a form of freedom, not least with regard to the prying eyes of the state. Isaiah Berlin spoke in his inaugural address at Oxford about two forms of freedom: positive and negative. Negative freedom—the demarcation of a space in which a person is free to do what she wishes and to be whom she wishes without outside interference—is linked to the keeping of secrets. It is the freedom to hold back information, even if there are others who want that information, or even claim to have a right to it. One definition of freedom is defined by being able and permitted to have secrets. If anyone needs to be convinced of this, I suggest you read Orwell's (1949/1989), which is more effective than any academic thesis. Here secrecy is related to privacy. If we use privacy to demarcate between public and private, we can connect this again to Berlin:

[12] Horn (2011: 117)

[13] Hacking (1990)

[14] Surveillance scholar Lyon (2007: 3) maintains that all surveillance 'moves somewhere on the continuum between care and control'.

[15] Prins et al. (2012); Lyon 2015

> It follows that a frontier must be drawn between the area of private life and that of public authority. Where it is to be drawn is a matter of argument, indeed of haggling.[16]

There is a struggle over where to draw the boundary, certainly in a time where our technological environment is designed to record our social and economic lives as data. What is our current era doing to the function and meaning of secrecy? What does it mean for individual and state secrets? From these two things also follows a third category of secrets that is growing more important in today's information society: the secrets of technology itself.

4 The Social Individual as the Transparent Individual

It is often said that privacy is dead. Over. Something of the past. The large internet companies have contributed to this. Scott MacNealy, one of the directors of Sun Microsystems, said already in 1999 at a press conference: 'You have zero privacy anyway. Get over it.'[17] The end of privacy is often ascribed to users themselves: they do not care about privacy any more. The urge to keep things secret is decreasing and young people are adopting new norms with regard to social behaviour. Research is showing, however, that the differences between age groups are more nuanced[18] and currently—against the background of the rise of Big Data, the Internet of Things and Snowden's revelations—privacy is becoming more valued. Privacy is also a legal instrument to protect information and secrets. But the way new technologies are becoming integrated into our daily lives makes privacy an ambiguous category.

For some applications, we have absolutely no secrets: we don't lie to our search engine. We are more intimate with it than with our friends, family and lovers. We always tell our search engine always exactly what we are thinking in the clearest possible terms.[19] Other applications tell on our secrets without our knowing it, or paying much attention. Our smart phones—the uncannily popular Judas of our times—constantly sends out our location, how long we spend there and which routes we take. Whoever likes to read books on Amazon's Kindle, may not realise that Amazon does not just know which book they are reading, but also how long you spend reading them, how fast you read and whether you finish a book or not. The Kindle sends all that information home to the mothership.[20] And because so much data collection is hidden behind consent forms, that make our digital lives so much more convenient, we click 'agree' more and more willingly.[21] We have absorbed the dominant business model of the internet fully into our daily lives: the user gets a free email programme, web browser, app or other service or product, and the provider hoovers up the digital details of the user's private activities, social contacts and networks. This creates a privacy paradox

[16] Berlin (1958)

[17] http://archive.wired.com/politics/law/news/1999/01/17538

[18] See for example: boyd (2014); Steijn and Vedder (2015)

[19] Schneier (2015: 22)

[20] In Schneier (2015: 28)

[21] Schneier (2015: 30) as surveillance fades into the background it becomes easier to ignore. And the more intrusive a system is, the more likely it is to be hidden. (…) In the near future, because these systems will be hidden, we may unknowingly acquiesce to even more surveillance. See also Zuiderveen Borgesius (2015) on the hollowing out of the concept of consent.

where most people say they are concerned about privacy, but behave in their everyday lives as if they do not care about it at all.[22] Despite the fact that a small number of users take different, and more anonymous, paths through the digital world, this does not seem to be good news for secrets in the information society.

The digital world is also a temptation for governments. There is more information than ever before and the possibilities for mapping out society are growing day by day: not only through the state's own data collection, but also indirectly through the wealth of information gathered by internet companies. 'Seeing like a state'[23] used to mean that governments observed the world through official statistics and registrations that they themselves collected on their people, their land and their properties. Although the state is not always the largest gatherer of data and personal details, within government organisation this information has become more fluid. Today's information government allows more information from its citizens to flow across the borders of ministries, registries, organisations and legal restrictions.[24] Also, the boundaries between public and private data become increasingly murky.[25] In some countries, the control of government over citizens in the digital society goes even further. In authoritarian regimes, attempts to control people extend to the minutiae of their online lives. Surveillance of communications and activities on the internet is business as usual for many authoritarian governments and is constantly being refined. [26] But in democratic countries as well, citizens are becoming more and more transparent to their own and to foreign governments. Even governments do their utmost to increase the transparency of their peers. The Snowden revelations showed that the American security agency NSA and other agencies gathered personal data on a global scale.[27] The rationale seemed to be that if you collect as much of the digital haystack as possible—'collect it all!'—so that the digital needle will probably come with it. This will have implications for the connection between citizens and government. For many citizens, it does not feel good that the government can see deep into your life and the past, and sometimes make predictions about your future on that basis.[28] The adage that 'he who has nothing to hide has nothing to fear' cannot quite remove the uneasiness. [29] Here, there is also a transparency paradox: the citizen becomes ever more transparent to the government, while it becomes increasingly complex for the citizen to understand which governmental organisations hold which information about him or her. The government, in other words, is becoming more and more opaque. That is also bad news for the citizen's ability to keep secrets in the information society.

We must ask, then, whether the individual is able to keep his secrets safe in the information society. Certainly with regard to the Goliaths that he is faced with: corporate as well as governmental. Companies such as Google and Apple have become, according to Bruce Schneier, the feudal overlords of the information society. [30] In exchange for

[22] Norberg et al. (2007)

[23] Scott (1998); see Taylor and Broeders (2015) on the issue of how commercially generated big data are used as a foundation for country-level 'data doubles', i.e. 'seeing like a state' through mostly private digital data and public-private cooperation in low and middle income countries.

[24] Prins et al. (2012)

[25] See for example Kitchin (2014)

[26] Deibert et al. (2008, 2010, 2011)

[27] Greenwald (2014)

[28] See for example Amoore (2013) and Pasquale (2015)

[29] See Solove (2011) for a thorough deconstruction of this argument

[30] Schneier (2013)

their products and services, we turn over our digital lives to them and deliver ourselves to the protection they offer. They determine our online security, access to our information and the level of privacy that they find proper. We have been manoeuvred into the position of the serfs of the digital age. They also shape our social world: 'Facebook defines who we are, Amazon defines what we want and Google defines what we think.' [31] Through this, social boundaries are constantly being redrawn: what is private, public and commercial? And what is secret now? Berlin's struggle over the boundary between what is public and what is private is being fought right here. The user, the citizen, or more simply the individual is increasingly transparent in the digital age. The city air breathes less free if you are overseen by cameras, your phone can be surveilled and your social networks can be laid bare in the most painful detail. If someone wishes to apply the full arsenal of the digital age to zoom in on an individual, as some companies and governments can do, they can throw light on dark corners that previously would have remained hidden. Simmel stated that someone who has no secrets and says everything out loud will probably keep few friends. How will the state—or its representatives—see citizens if it can mine so much information about them? 'Unknown makes unloved', goes a Dutch saying. Simmel suggests that the opposite will also encounter limitations: knowing more about someone does not per se make them more loveable. Harvard's Yochai Benkler has said recently that imperfection is a core dimension of freedom[32], something that relates well—albeit in the negative sense—to the desire of governments and corporations to know everything possible about everyone. For the individual, then, this means that secrecy must be saved from transparency.

Although digital society offers many opportunities to throw sand in the works and oppose what is going on[33], large-scale revolt is very unusual. If we see secrecy as a form of freedom, then we should also agree with Berlin's assessment that the struggle for Freedom with a capital F, in the sense of an abstract value is the struggle of a vanguard. In this, NGOs such as the Electronic Frontier Foundation and Bits of Freedom and hacktivist organisations such as WikiLeaks and Anonymous are in the lead, sometimes within and sometimes (well) over the limits of the law. Many people are prepared to offer their freedom on the altar of benefits such as security, welfare, power or another item from a long list of more and less noble goals and values[34], such as convenience in the information society. Google, which dominates 90 % of the European search engine market[35], has become the irresistible bargain offer of the European information society. Alternatives are available, but are still fairly modest in their offerings and market share. The digital world offers a wealth of information and communication, but the user contributes as well. As the internet economy cliché goes, 'if something is free, you are not the customer, you are the product'. The debate about the limits of this exchange and the question as to what the boundary between private and public should be will only become more important in the coming years.

[31] Dyson (2012: 308)

[32] See: http://harvardmagazine.com/2013/12/security-versus-freedom

[33] See for example Marx (2003); Brunton and Nissenbaum (2011)

[34] Berlin (1958): The bulk of humanity has certainly at most times been prepared to sacrifice this [freedom, DB] to other goals: security, status, prosperity, power, virtue, rewards in the next world; or justice, equality, fraternity, and many other values which appear wholly, or in part, incompatible with the attainment of the greatest degree of individual liberty, and certainly do not need it as a precondition for their own realisation."

[35] http://uk.businessinsider.com/heres-how-dominant-google-is-in-europe-2014-11?r=US&IR=T

5 The State's Secrets

What does the information society do for the state's secrets? Simmel's expectation was that the state would become more open and transparent under the influence of modernisation. The answer seems to be mixed: state secrecy expanded in many countries over the twentieth century, but digitisation—which positions the government to peer deep into the lives of its citizens—also forces the state to look at its own practices of secrecy.

State secrecy exists between two extremes. On the one hand, secrets, as noted earlier, are a form of power. This was encapsulated by Hannah Arendt as 'real power begins where secrecy begins'.[36] On the other hand, the state simply needs secrecy to fulfil some of its tasks and duties towards society, for example in the case of national security. In the words of William Colby—a former director of the CIA—'Secrets are necessary to a free society.'[37] The choice, in other words, is not black and white. Drawing an appropriate boundary between what the states may keep to itself and what should be shared with citizens, then, is extremely important.

In contrast to Simmel's expectations, the modern state has not lost its appetite for secrecy. The American security agency NSA, over which there has been much to do, was set up in 1952 by a secret presidential directive from Harry Truman. The organisation and its mission remained secret until a scandal in the 1970s 'outed' the organisation to the general public.[38] In general, states have the tendency to keep more information secret and to classify more. In the US Bruce Schneier speaks of a secrecy creep, and proposes that secrecy has exploded.[39] But in Europe too, secrecy is gaining rather than losing ground. Legal scholar Deirdre Curtin shows how secrecy regarding documents in the EU is on the rise, and especially within the domain of Justice and Home Affairs. She speaks of a culture of secrecy that leads to a rampant culture of overclassification. In America this is no small problem—experts estimate that 50–90 % of the classified material in government is overclassified, or should not be classified at all.[40]

States naturally want to make sure that anything marked as secret, stays secret. In the digital society that is no simple task. If the NSA at the start of its existence was a good example of an *arcanum*—no one knew that it existed—since 2013 it has become a *secretum* that is cracking at the edges. The digital era also puts government secrets at risk. Private Chelsea—at that point still Bradley—Manning copied around 250,000 secret documents from the US State Department onto a DVD on which he had written 'Lady Gaga' in pen, and handed it over to the whistleblowers at WikiLeaks.[41] Edward Snowden did not even work for the American government but for Booz Allen Hamilton, an American consulting firm that worked for the NSA. How many documents he took from the NSA's servers is unknown, but according to Keith Alexander, then director of the NSA, the number could be as high up as a million.[42] The era of Big Data, then, also

[36] Arendt (1973: 403)
[37] Colby (1976: 4)
[38] Glennon (2014: 75)
[39] Schneier (2015: 99)
[40] Curtin (2011:18–19)
[41] http://www.theguardian.com/world/2010/nov/28/how-us-embassy-cables-leaked
[42] http://www.afr.com/technology/web/security/interview-transcriptformer-head-of-the-nsa-and-commander-of-the-us-cyber-command-general-keith-alexander-20140507-itzhw

applies to the leaking of government secrets. No one can get 250,000 paper documents out of the building unseen, but with bits and bytes, it is another storey.

This means that states need to think hard about how to keep secrets in the digital age. Peter Swire, a member of the commission tasked by President Obama with looking into the functioning of the US intelligence services[43], has said that in the digital era, secrets are not likely to remain secrets for as long as they used to. He called this the 'declining half-life of secrets'.[44] Technological advances, the fact that intelligence services work in public-private partnership far more often (instead of relying on employees with a self-professed lifelong calling), and the multiplicity of sources they use, make the secrets they keep vulnerable. The collection of information is less the issue than keeping secret the fact that you are collecting it, which is getting much more difficult. And it matters a great deal politically whether today's paper publishes the storey that German Chancellor Willy Brandt was wiretapped by the Americans in the 1970s, or a storey that the same is done to Angela Merkel, the current German Chancellor, who will pick up the phone to call the White House.

For the state, then, it seems that the secret must be saved from over classification and secrecy itself. Perhaps it is the nature of the information society that will force the state to make hard choices about state secrecy. Otherwise the enthusiasm for gathering and keeping secret information threatens to overwhelm the legitimate function of state secrecy. That suggests that democratic constitutional states need to take a serious look at what the government really wants to categorise and treat as secret. For the collection of personal data there is the privacy mantra, 'select before you collect', and for secrecy maybe there should be a government mantra of 'select before you protect'.

6 Technology's Black Box

The last secret is concealed within technology itself. Modern information technology, which puts pressure on individual as well as state secrecy, also has its own secrets. It is a commonplace in the *Science and Technology Studies* literature that technology is not a neutral instrument. Technologies have their own dynamics and interact with their social environment. Technology is often seen as a black box. What exactly happens inside it is not so easy to figure out. A good example of a black box technology in the time of big data is the use of algorithms in the analysis of large-scale databases. At a time when the amount of data is growing exponentially and is expected to create both economic profit and new knowledge, algorithms are essential. An algorithm is a specific series of steps that turn input data into outputs: it generates an output. An algorithm processes a given dataset in order to draw information out of it: from your Google search results and the Amazon books that fit your preferences to the potential fraudsters and terrorists in government data analytics. Programming algorithms involves coding in choices: which data should be picked up or not, which categories and profiles should be created, and how they should be weighted. These choices are made by people—designers and programmers—and increasingly also by algorithms themselves. Algorithms are increasingly capable of learning, something termed deep

[43] Clarke et al. (2013)

[44] Swire (2015)

learning or machine learning, and as they are allowed to process increasing amounts of data—which is the case with big data—they become themselves more complex. Google search does not work through a single algorithm, but around 200 that together determine what comes up first in your search results. These algorithms are becoming ever more important in our daily lives: Google's algorithm determines how I see the world, and those of the intelligence and security services determine whether I am seen as a risk.

Algorithms themselves are often secrets. Firms categorise them as corporate secrets and governments classify them because they create insight into their method of operation.[45] They are kept secret because sharing them creates the risk of people gaming the system. If you know what they are searching for, you can avoid that pattern—like the criminal or fraudster who escapes digital capture. Or, reversely, you can embrace the pattern—like the website that wants to appear at the top in the page with search results. The thriving market for so called 'search engine optimization' is testimony to the reality of gaming the system. This secrecy however obscures all the choices, weightings of risk and other values that combine in the algorithm and database. They are shut away from view and cannot be questioned. From outside, it looks as if there is a closed system that produces results with mathematical precision and authority. Bowker and Star write in their classic work on classification that information architecture—and the politics that lie hidden within it—is hard to analyse:

> Good useable systems disappear almost by definition. The easier they are to use, the harder they are to see. As well, most of the time, the bigger they are, the harder they are to see.[46]

The big black boxes—and all the secrets that they enclose—disappear behind the façade of a good useable system. How their results are produced becomes obscured, while the effect of those results on people's lives keeps growing. 'Computer says no' is the digital version of the *deus ex machina*.

Modern digital technologies, then, have a mystery, literally in the sense of the *mysterium* as discussed earlier. That is something that has changed little over time. At the beginning of the twentieth century, Max Weber discussed the disenchantment of the world.[47] Rationalising society would, according to him, take the mystery out of the world because new technologies 'can, in principle, master all things by calculation'.[48] That is not to say that Weber thought modern technology itself was comprehensible for anyone. He argued instead that there was a 'knowledge or belief that if one but wished one could learn it at any time'. In practice, however, disenchantment would lead to division of labour and specialisation of knowledge meaning that most people did not understand how a lift, tram or computer worked. That was for experts. Freely translated to our digital age: for most people ICT is a mystery, but for experts the zeros and ones of the algorithm have no secrets. According to sociologist Stef Aupers, however, this is

[45] Pasquale (2015); Gillespie (2014)

[46] Bowker and Star (2000: 33)

[47] Weber (2004: 12–13)

[48] 'That in turn means the disenchantment of the world. Unlike the savage for whom such forces existed, we need no longer have recourse to magic in order to control the spirits or pray to them. Instead, technology and calculation achieve our ends. This is the primary meaning of the process of intellectualization.' Weber (2004: 13).

not the case. The ICT specialists that he interviewed in Silicon Valley all emphasised ‘the opaque and unpredictable nature of contemporary digital technology’.[49] For these experts too, the mystery of technology seems to be greater than commonly assumed. The simplicity and tranquillity of the Google home page conceals around 200 algorithms. The number of people at Google who can see all of them, and understand them, is probably extremely limited. It would not surprise me if there were none. But it is, in the words of Bowker and Star, a good useable system. But certainly, one that has its own secrets.

7 Conclusion

The secret is a somewhat forgotten but vital sociological theme into which we should enquire more, especially in light of the fast changes in our digital society. With more and more of our lives lived and/or tracked online, the future of secrecy is not bright. Simmel’s enthusiasm—the secret is one of man’s greatest achievements—has an oppressive echo in the words of Sissela Bok: ‘With no control over secrecy and openness, human beings could not remain either sane or free.’[50] Spiritual health and freedom are high stakes that merit more of an academic effort to understand and think through the political and social complex of digitisation, secrecy, privacy and transparency.

References

Amoore, L. (2013). *The politics of possibility. Risk and Security Beyond Probability.* Durham and London: Duke University Press.

Arendt, H. (1973). *The Origins of Totalitarianism*. San Diego: Harcourt.

Aupers, S. (2009). The force is great: enchantment and magic in silicon valley. *Masaryk University Journal of Law and Technology, 1*(1), 153–173.

Berlin, I. (1958/1969). *Two concepts of liberty. Four essays on liberty.* New York: Oxford University Press.

Bok, S. (1989). *Secrets: On the Ethics of Concealment and Revelation*. New York: Vintage Books.

Bowker, G., & Star, S. (2000). *Sorting things out. Classification and its consequences*. Cambridge, Massachusetts: The MIT Press.

Boyd, D. (2014). *It’s complicated. The social lives of networked teens*. New Haven: Yale University Press.

Broeders, D. (2015) Het geheim in de informatiesamenleving. Oratie Erasmus Universiteit Rotterdam, 30 October 2015.

Brunton, F. en H. Nissenbaum (2011) "Vernacular resistance to data collection and analysis: A political theory of obfuscation." First Monday 16 (5). Available at http://firstmonday.org/htbin/cgiwrap/bin/ojs/index.php/fm/article/viewArticle/3493/2955.

Clarke, R., M. Morell, G. Stone, C. Sunstein and P. Swire (2013) Liberty and security in a changing world. Report and Recommendations of The President’s Review Group on Intelligence and Communications Technologies, 12 December 2013. https://www.whitehouse.gov/sites/default/files/docs/2013-12-12_rg_final_report.pdf.

[49] Aupers (2009: 169)

[50] Bok (1989: 24)

Colby, W. (1976). Intelligence secrecy and security in a free society. *International Security, 1*(2), 3–14.

Craib, I. (1997). *Classic Social Theory*. Oxford: Oxford University Press.

Curtin, D. (2011) Top secret Europe. Inaugurele rede Universiteit van Amsterdam, 2011.

Deibert, R., J. Palfrey, R. Rohozinski and J. Zittrain eds. (2008). Access Denied: The practice and Policy of Global Internet Filtering, Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski and J. Zittrain eds. (2010). *Access Controlled: The Shaping of Power, Rights, and Rule in Cyberspace*, Cambridge (Mass.): MIT Press.

Deibert, R., J. Palfrey, R. Rohozinski and J. Zittrain eds. (2011). *Access Contested. Security, Identity, and Resistance in Asian Cyberspace*, Cambridge (Mass.): MIT Press.

Dyson, G. (2012). *Turing's Cathedral. The origins of the digital universe*. New York: Vintage Books.

Gillespie, T. 2014. "The Relevance of Algorithm." pp. 167–94 in. T. Gillespie, P. Boczkowski, and K. Foot (eds.) *Media Technologies: Essays on Communication, Materiality, and Society*, Cambridge (Mass.): MIT Press.

Glennon, M. (2014). National security and double government. *Harvard National Security Journal, 5*(1), 1–114.

Greenwald, G. (2014). *No Place to Hide. Edward Snowden, the NSA and the US Surveillance State*. New York: Metropolitan Books.

Hacking, I. (1990). *The taming of Chance*. Cambridge: Cambridge University Press.

Horn, E. (2011). Logics of political secrecy. *Theory, Culture and Society, 28*, 103–122.

Kitchin, R. (2014). *The data revolution. Big Data, open data, data infrastructures and their consequences*. Londen: Sage.

Lyon, D. (2007). *Surveillance Studies. An overview*. Cambridge: Polity Press.

Lyon, D. (2015). *Surveillance after Snowden*. Cambridge: Polity Press.

Marx, G. (2003). A tack in the shoe: neutralizing and resisting the new surveillance. *Journal of Social Issues, 59*(2), 369–390.

Marx, G., en G. Muschert (2009) "Simmel on secrecy. A Legacy and Inheritance for the Sociology of Information.", pp. 217–233 in. C. Rol and C. Papilloud (eds.) *Soziologie Als Möglichkeit: 100 Jahre Georg Simmels Untersuchungen Über Die Formen Der Vergesellschaftung*. Wiesbaden: VS Verlag für Sozialwissenschaften.

Norberg, P., Horn, D., & Horne, D. A. (2007). The privacy paradox: personal information disclosure intentions versus behaviors. *Journal of Consumer Affairs, 41*(1), 100–126.

Orwell, G. (1949/1989) *Nineteen eighty-four*. London: Penguin Books.

Pasquale, F. (2015). *The Black Box Society. The Secret Algorithms That Control Money and Information*. Cambridge: Harvard University Press.

Prins, J. E. J., Broeders, D., & Griffioen, H. (2012). iGovernment: a new perspective on the future of government digitisation. *Computer Law & Security Review, 28*(30), 273–282.

Quill, L. (2014). *Secrets and Democracy. From Arcana Imperii to Wikileaks*. New York: Palgrave Macmillan.

Schneier, B. (2013) 'Power in Age of the Feudal Internet', pp. 10–14 in U. Gasser, R. Faris and R. Heacock (eds.) *Internet Monitor 2013: Reflections on the Digital World*, Cambridge (Mass.): The Berkman Center for Internet and Society.

Schneier, B. (2015). *Data and Goliath. The Hidden Battles to Collect Your Data and Control Your World*. New York: W. W. Norton & Company.

Scott, J. (1998). *Seeing like a State. How certain schemes to improve the human condition have failed*. New Haven: Yale University Press.

Simmel, G./K. Wolff (1950) *The Sociology of Georg Simmel*. Translated, edited and with an introduction by Kurt. H. Wolff. New York: The Free Press.

Solove, D. (2011). *Nothing to hide. The false trade off between privacy and security*. New Haven: Yale University Press.

Steijn, W., & Vedder, A. (2015). Privacy under construction: a developmental perspective on privacy perception. *Science, Technology & Human Values, 40*(4), 615–637.

Swire, P. (2015). *The Declining Half-life of Secrets and the Future of Signals Intelligence. New America Cyber Security Fellows Paper Series no. 1, July 2015*. Washington: New America Foundation.

Taylor, L., & Broeders, D. (2015). In the name of development: power, profit and the datafication of the global south. *Geoforum, 64*(4), 229–237.

Weber, M. (2004). *The vocation lectures.* "*Science as a vocation*" *and* "*Politics as a vocation*". Indianapolis: Hackett Publishing Company.

Zuiderveen Borgesius, F. (2015). *Improving Privacy Protection in the Area of Behavioural Targeting*, Alphen aan den Rijn: Kluwer Law International.