ephemera
theory & politics in organization

ISSN 1473-2866 (Online)
ISSN 2052-1499 (Print)
www.ephemerajournal.org
volume 19(4): 777-806

Citizen duty or Stasi society? Whistleblowing and disclosure regimes in organizations and communities

Steven Sampson

abstract

This paper argues that the concept of whistleblowing could best be understood as part of a larger regime of disclosure that includes personal revelations, truth-telling, leaking, informing, snitching and whistleblowing. Disclosure regimes are about knowledge that escapes. This paper discusses the conditions for this escaped knowledge and some of the consequences for organizations and communities. Two examples of disclosure regimes are provided: first, the US Government's financial rewards for whistleblowing, in which disclosed knowledge of company wrongdoing can be packaged for company sanctions and courtroom litigation; and second, Scandinavian community informing programs where citizens can anonymously inform authorities of neighbours' suspected welfare cheating or tax evasion. The examples of knowledge that escapes show disclosure regimes to be a field in which organizational or community loyalties confront employee/citizen duties, cultures of organizational/community solidarity and the ethos of non-interference/privacy. As new disclosure regimes and practices evolve, thanks to massive financial rewards, encouragement of transparency and anonymous technologies, we will need to redefine what whistleblowing is all about. A focus on disclosure regimes can help reveal the inner workings of organizations or communities, as knowledge managing groups.

Introduction

Organizations channel resources to achieve goals.[1] In doing so, they must organize knowledge. This organizational knowledge is distributed within strict hierarchies, specialized sections, flexible teams or informal cliques. Whistleblowing disrupts this knowledge distribution. In our conventional understanding of whistleblowing, an employee or someone with inside knowledge discovers certain practices, known in the literature as 'wrongdoing', and discloses knowledge of these practices to someone outside the knowledge hierarchy: an unaware superior, the company's ethics unit, or an outside authority. These recipients of knowledge should somehow rectify the wrongdoing (Near and Miceli, 1985, 1996; Miceli et al., 2008). In addition to this specific correction process, disclosing knowledge of illicit practices also sets in motion other connected processes. There may be retaliation against the truth-teller/whistleblower, unwanted publicity for the firm, branch-level reform measures and legal sanctions imposed by the outside authority. Research on whistleblowing, operating with a definition grounded in organizational life, has understandably focused its attention on knowledge escape within organizations and on how the whistleblower decides to disclose knowledge (e.g. Miceli et al., 2008). The standard approach to whistleblowing as something that occurs within organizations has its merits, since all scientific concepts need to be demarcated in order to be analytically useful. Yet the disclosure of knowledge is not just something that happens to organizations or firms. Knowledge can escape in different forms, only one of which is whistleblowing. Social life of all kinds is predicated on combinations of knowledge control and knowledge distribution processes. In families, for example, private, intimate, or scandalous knowledge should be kept within the family; it should not reach the neighbours or the gossip pages. In a community, the affairs and conflict within the group should be confined to bona fide community members. In social groups or tribes, the sacred tribal knowledge should be held in trust by the tribal elders. Initiation rites in lodges or tribes are in fact the disclosure of secret or sacred knowledge to others. In all kinds of settings, the penalties for unwittingly discovering or deliberately disclosing this kind of knowledge to outsiders can be severe, whether it be an initiation right in a lodge, or a secret tax shelter of a company. Every organization, community, or social group has its own type formal or informal 'non-disclosure agreement'. Every social group endeavours to ensure that their

1 An earlier version of this paper was presented at the 2017 American Anthropological Association Annual Meeting in Washington, DC in our panel 'Beyond Snowden: The Anthropology of Whistleblowing', where I received valuable comments from participants. I would also like to thank Richard Weiskopf and the anonymous reviewers at *ephemera* for their detailed critiques and suggestions on previous editions of this paper.

private, internal, confidential, sensitive, secret or sacred knowledge does not reach the wrong people, be they the uninitiated, outsiders, authorities, or the media. Unauthorized disclosure (via espionage, leaking, hacking, unwitting dissemination or whistleblowing) is a threat to those who consider themselves the guardians of the firm/family/tribe/group. Knowledge must be protected or controlled. Escaping knowledge is dangerous.

As we know, many such efforts to control, protect and restrict knowledge often fail. Family secrets get discovered; corporate slush funds are revealed, etc. We live in an age of disclosure. At the personal level, many of us now revel in revealing our most private thoughts or anxieties to strangers, colleagues or online 'friends'. Social media is filled with people unburdening their revelations, confessions, projects, successes, failures, addictions, gossip and accusations. Aside from voluntary disclosures of this kind, other knowledge is unwittingly leaked, aggressively stolen or coerced out of us by hackers, authorities and threats. This escaped knowledge thrives in an age when the pursuit of transparency, here understood as seeing through the surface or revealing the hidden essence, is a moral imperative (Sampson, 2019). We are encouraged to be transparent ourselves, to disclose voluntarily (Heemsbergen, 2016) or to shine the flashlight on suspicious practices, in what one scholar has called 'the tyranny of light' (Tsoukas, 1997). Whistleblowing, and the cult of the whistleblower (the hero who reveals secrets and who needs protection from retaliation), is thus part of this disclosure and transparency configuration. Not all disclosed knowledge achieves its intended impact – politicians can brush off accusations or shoot the messenger (or put them in prison or exile, as Assange, Manning and Snowden can attest). Yet modern life, both in organizations and generally, is now dominated by the contradictory efforts to prevent knowledge from escaping and by the push toward disclosure, be it disclosure motivated by personal revenge against an employer or disclosure in pursuit of some kind of transparency ideal. We live, I would assert, within overlapping 'disclosure regimes', in which pressures for secrecy and confidentiality, to respect formal and informal non-disclosure agreements, are threatened by the prospect of escaping knowledge. Those who guard knowledge never know when that secret file, the confidential e-mail, the suspicions bank transaction, the immoral relationship, the unauthorized favour, or the untoward practice will come to the attention of others outside our circle. Not all this disclosure is of earth-shattering significance, of course, as gossip magazines show. But both the various imperatives toward openness and transparency (Han, 2015) and the perceived benefits that people can derive from obtaining and curating escaped knowledge serve to prop up these disclosure regimes. No knowledge is safe.

We will find disclosure regimes emerging in situations and sites where our ties to 'our' organizations or communities are more tenuous, or where sanctions that could have been brought to bear (tradition, discipline, unquestioned authority, fear) are not as effective. In the era of flexible employment, workers have less loyalty toward their organizations; whistleblowers, even if threatened, now have some 'rights' or at least 'protection from retaliation'. Thanks to anonymous digital platforms, more knowledge can be procured and can escape more easily (no more nights at the photocopy machine, just get the right password and click 'send'). Hence, for every effort by firms or organizations to upgrade their secrecy and confidentiality, for every additional level of 'need to know', there also appear new opportunities for disclosure, new channels to distribute the escaped knowledge, new ways to valorise this knowledge and new potential recipients 'out there'. Not a day passes when we do not have new revelations, new accusations, new disclosures, from *MeToo* to municipal kickbacks to embarrassing videos to the thousands of pages of an offshore law firm that were the Panama Papers.

In this buzz of disclosures, I wish to suggest that we view whistleblowing as part of a much larger set of practices which cross-cuts not only firms and organizations but which also includes social groups, communities, neighbourhoods, or associations. The disclosure practices that we call whistleblowing resemble similar processes that take place in other social groups, all of which consist of 'knowers' (Barth, 2002). What we call 'organizing', therefore, is not just the disciplining of groups or persons to achieve goals. Organizing is the actions of people who organize, control, dispense and re-distribute knowledge. Shared knowledge is what makes groups, associations, organizations or firms. But under certain conditions, this intimate knowledge either escapes through the wrong channel (an unauthorized leaker) or is purposely disclosed by someone who is supposed to keep the knowledge secret (the gossiper, the accountant, the vengeful whistleblower). This kind of unauthorized dissemination of knowledge has greatest impact when it reveals gaps between the ideally proclaimed and actual practices of social groups, as gaps of this kind call into question the moral foundations of the firm, organization or group. Escaping knowledge is thus a moral, even existential threat (as the Catholic Church paedophile scandal shows).

I call this set of practices surrounding the escape of knowledge a 'disclosure regime'. These practices are limited to the unauthorized distribution of knowledge, i.e., knowledge escaping. As such, disclosure regimes operate under various types of incentives. The knowledge can originate and flow over different channels, there can be diverse content, and the escape of knowledge can have varying outcomes for both the 'knower' who reveals and for the recipients. Disclosure regimes thus have an 'order', in the sense that they are not simply

deviant or chaotic. They are the underside, the mirror image of formal knowledge regimes. They are a type of knowledge *mis*management, what might be called 'renegade knowledge'. Let me give a simple example of a possible disclosure regime within a firm. Here the most benign kind of escaping knowledge might be corridor gossip about the firm's financial manager who has suddenly been fired. Were the content of the gossip to change from the manager's unexplained firing to the fact that this same manager was responsible for the firm's illegal tax shelter, and were the information heard in the corridor to be transmitted to the FBI's white collar crime hotline, then the benign 'gossip' would become more threatening 'whistleblowing'. And if this whistleblowing information were packaged in such a way, perhaps with the help of a lawyer, into a legal complaint, we would have the possibility of a trial, with the resulting bad publicity for the firm, financial compensation paid to the whistleblowing employee, and possible retaliation by the firm for breaking a non-disclosure agreement. It is in scenarios such as this that show how disclosure regimes in firms have a special constellation of features. We could outline sets of incentives, types of information, channels of transmission, and various impacts, including the way authorities and organizations react.

In this paper, therefore, I will show how disclosure regimes (the practices surrounding the escape of knowledge) can be compared. In this sense, I will seek to show that whistleblowing in organizations is only one moment in one kind of regime. Hence, whistleblowing can be compared to other ways in which knowledge escapes, which may be different in other kinds of disclosure regimes. We can sketch out the variations in which escaping knowledge can be selected, conveyed, packaged, curated, rewarded or sanctioned. I will therefore begin by outlining some further general characteristics of a disclosure regime, attempting to show why an understanding of 'knowledge that escapes' may be useful in studying whistleblowing. In this way, we may also help elucidate the oft-discussed question of why so much illicit behaviour in firms is still not reported. I then discuss in detail two types of disclosure regimes: firstly the U.S. Government whistleblower reward system used by several agencies to expose corporate financial wrongdoing or corruption; and secondly, the citizen 'snitch' system in Denmark and Sweden, in which citizens can anonymously inform local authorities of neighbours whom they suspect are cheating on welfare benefits or taxes. By comparing two kinds of disclosure regimes, one that subsumes corporate whistleblowers, the other in Nordic welfare states, one that gives rewards, the other that allows personal revenge, we can better understand the broader issue of how 'organizing' works, how knowledge is managed, and what happens when knowledge escapes. Let me therefore provide more clarification of what disclosure is all about.

What is a disclosure regime?

A disclosure regime is a set of practices which formally or informally regulate the escape of knowledge. This 'regulation' can take the form of preventing, encouraging, rewarding or punishing such escaped knowledge. (I use the term 'regime' here because even though disclosure practices may begin as informal or unofficial, they invariably interact with some kind of institutional or regulatory authority, such as a council of elders, courts or a local government; terms such as 'disclosure assemblage' or 'disclosure complex' might serve equally well). Disclosure regimes operate in all kinds of social groups. This is because social groups are held together by organizing their 'resources', and one of these resources is knowledge. Every system of knowledge control – whether embedded in a family, a firm, an association, a club, a bureaucracy, an intelligence agency, or a group of tribal elders – attempts to keep certain kinds of knowledge within closed circles, as confidential or secret. The closed/secret nature of this knowledge makes it attractive, or even valuable, to others. Knowledge-handlers selectively release or dispense certain knowledge in order to maintain power, show status, or neutralize rivals. If power is about control over knowledge, a disclosure regime dilutes this kind of power by regulating how knowledge escapes. The incentive to disclose intimate knowledge may be a combination of personal compulsion, revenge or external reward. Someone in the know, or with access to knowledge, discloses this knowledge beyond the group. The 'escaped knowledge', such as a leak or whistleblowing, alters vectors of power and influence. The escape of knowledge, is a special moment in an organization's life; once the disclosed knowledge becomes widely known, its value changes; the well-kept secret may become 'old news' and quickly forgotten; or it becomes recurring 'gossip' in a magazine; or it may be a scandal that must be cleaned up using image experts; or the knowledge may become a more radical 'game changer' for the organization, compelling it to reorganize itself; or it may become damning evidence in a trial, bringing down the firm entirely (e.g. Enron and Arthur Andersen).

One final aspect of disclosure is its pervasive character. Like transparency, escaped knowledge seems to overflow its bounds, existing as a potentiality in any group. Hence, the very threat of disclosure will be part of the daily environment for those whose task is to ensure control over knowledge, much like we all now fear someone hacking into our personal computer and emptying our bank account. This potentiality of disclosure is especially serious for knowledge that may be deemed morally suspect or legally objectionable, i.e., the kind of escaped knowledge that reveals discordances between declared ideals/morality and actual practices (e.g., sexual abuses in the Catholic Church, in Hollywood, in the Swedish Academy, or in the illicit financial dealings in the Panama Papers or

Danske Bank). A disclosure regime thus operates with a range of possible incentives, carriers of knowledge, content of knowledge, potential channels of conveyance, and of course, numerous possible outcomes and impacts, ranging from financial reward, good or bad publicity to both the knower and the organization, or retaliation against the teller of secrets or the whistleblower.

A disclosure regime does not mean that we live in an era of total transparency. Secrecy and transparency are in constant confrontation, as all social life and organizational operations depend on certain amounts of personal privacy and organizational confidentiality (Birchall, 2011). On the transparency side, activist groups, the media and the public are preoccupied with uncovering restricted knowledge. On the privacy side, firms fearing escape of their knowledge now emphasize their rights to privacy, secrecy, confidentiality and non-disclosure agreements. At the individual level as well, we are all trying to protect ourselves from the impositions of marketing firms, hackers or government organs who are trying to learn about our daily habits and intimate lives. We do not want knowledge about our private life to fall into the wrong hands. In this nexus of knowledge control and knowledge escape, of privacy protection, fear of surveillance, transparency pressures and disclosure threats, two contesting issues emerge: Those who have seen their knowledge escape ask, 'How did they find out?' or 'Who told the secret?'. And for those who have discovered or been given access to this escaped knowledge, the issue is 'Why didn't we know about this earlier?'. This confrontation between those pursuing secrecy versus those pursuing transparency leads to political projects of renewed knowledge control (more surveillance of potential leakers in firms, more data privacy for individuals), followed by renewed campaigns of transparency and mandatory 'reporting' regulations (about sustainability, registration of financial transactions, listing of number of complaints handled, setting up hotlines, public lists of sexual offenders, etc.). Disclosure practices thus create and are then subjected to political pressures, policy guidelines, statistical indices and regulatory discipline. In this way, certain informal disclosure practices become institutionalized. They become genuine 'regimes' with the governance discourses these entail. The emergence of whistleblower protection laws covering ever greater sectors of both business and the public sector is one example of this institutionalization of disclosure regimes (Olesen, 2019; Vandekerckhove, 2006). Sexual harassment hotlines are another. To take one more example: in Norway and Sweden, two societies which value individual privacy, public pressure about unequal incomes has led to a situation where anyone can find out about anyone else's individual incomes and their mortgage loans. In a disclosure regime, politicians and officials who once had to deal with requests to release information on a case by case basis must now justify why they do *not* release all information at once. Knowledge based on 'need to know' is replaced by the pressure of 'public

interest' or the requirement to justify nondisclosure. I argue that we have reached a kind of tipping point in the struggle between knowledge control and disclosure, where disclosure is getting the upper hand, even as individual disclosure actors are imprisoned or in exile.

Disclosure practices take place within the tense relation between employees and employers, between citizens and the state, and between people and each other inside workplaces or communities. In this sense, whistleblowing lies on a continuum of disclosure practices that extend from personal confessions, revelations of being abused by others, the leaking of illicit secrets to the press or state authorities, to informing on one's workmates and neighbours for individual gain or revenge, to the radical disclosure of the hacker, and to the organizational dissidence that we know as whistleblowing. This continuum of disclosure practices may be found in many disclosure regimes and in different variants. Hence, few scholars would describe the Scandinavian case of neighbour informing as whistleblowing, in so far as the conventional definition of whistleblower revolves around the organizational insider who reveals knowledge of wrongdoing. On the other hand, whistleblowers are often accused by their colleagues of breaking a private loyalty, of being 'snitches'. Snowden, for example, is a whistleblower only for those who support him; for others he is a criminal. Similarly, it seems equally awkward to view the Scandinavian homeowner who sees his neighbour abusing the welfare system as some kind of snitch or 'informer' of the Stasi variety. The Stasi informer collaborated with the secret police, perhaps for some reward. The Scandinavian 'snitch' is presumed to have some higher mission, to redress an illicit practice; in this case welfare abuse. There is no reason why police informer and whistleblower systems could not exist simultaneously, as they in fact did in the Soviet Union (Lampert, 1988). The decisions by ordinary Danes and Swedes to inform authorities about the illegal practices of their neighbours has many elements of the whistleblowing process (identification of wrongdoing, the decision to report, the reaction of authorities). Like whistleblowing, the motives for informing may range from a feeling of civic duty to simple envy or revenge, again echoing the contrast between personal, private and public motives in the whistleblowing literature (see also Roberts, 2014). Calling Scandinavian informing Stasi-like, as some Danes have done, would therefore be a misnomer. The point here is that both whistleblowing and informing are part of different disclosure regimes and are perhaps better understood as part of a disclosure continuum. Using the two examples, I will try to show that organizational whistleblowing and Scandinavian informing may have some underlying commonalities, especially as regards loyalty and integration in social groups. Both could be viewed within a larger framework of escaping knowledge, or knowledge mismanagement if you will. This is because it is not just organizations or firms that exercise 'knowledge

management'. So do communities, neighbourhoods and social groups of all kinds. Where there is such management of knowledge, we can thus expect instances of knowledge mismanagement, of knowledge that escapes in the form of whistleblowing, snitching, revelations, and leaks. All can be found in various disclosure regimes.

Disclosure regimes themselves do not mean we are a better informed society (Flyverbom, 2016; Flyverbom and Albu, 2017). Unauthorized release of information (what Heemsbergen (2016) calls 'radical disclosure') still requires that the liberated knowledge be digested, interpreted and utilized before it becomes useful. Snowden, for example, did not give us 'knowledge', he released data dumps (Gladwell, 2016). It was only when the data was analyzed that we gained the political knowledge that the National Security Agency was spying on American citizens; the outcome of this release of knowledge remains unclear, not just for Snowden, but for the U.S. political system.

Escaped knowledge does not travel in a vacuum. The knowledge becomes linked to or appropriated by other actors who try to manipulate it for their own ends. In this sense, disclosure creates new kinds of knowledge control processes. Private firms and government agencies now employ an army of communications specialists whose task is to control knowledge. They monitor employees' communication, search for leaks, confront whistleblowing accusations, deal with freedom of information requests, handle employee complaints and threats to go public, and make strategic disclosures of sensitive information before it escapes through the wrong channels. In so far as knowledge is about seeing, we might regard this frantic activity of knowledge control as 'visibility management' (Flyverbom, 2016) supplemented by 'voluntary disclosure' (Heemsbergen, 2016). Two tendencies cross paths: first, firms, organizations and individuals want to restrict, or in any case curate, what others know about themselves/ourselves. They thus restrict or package the knowledge in discreet or obtuse ways. Second, individuals or partisan actors are searching out knowledge that is 'ripe for escape' and then disclosing this knowledge outside the legitimate channels: Snowden gave his data to the journalist Glenn Greenwald, others give or sell their knowledge to WikiLeaks, gossip columns, marketing firms, law offices, or intelligence organs. Organizations and groups need to conceal some knowledge for normal or special operations while confronting the pressures for disclosure based on an ethos of transparency or to alleviate suspicion.

With the concept of disclosure regime, we can understand the kinds of knowledge that are embedded in various kinds of social units. We can investigate not just who has access to knowledge but also who discloses what to whom. This kind of approach requires us to discover how knowledge within organizations or

other social groups is generated, managed and distributed, and to identify how knowledge can escape from its social framework. In a firm, the insider-whistleblower is one channel of such knowledge escape. Another is the police informer sent in from outside. A third is the concerned citizen who discovers abuse. A fourth is the individual who reveals their own victimization in the hope that others will also come forward. Other channels can be listed, of course, but my point here is to view whistleblowing in organizations within a larger disclosure-based framework.

Two case studies of disclosure regimes

Here I wish to provide two examples of how the process of disclosure might operate. In both cases, knowledge of internal or private wrongdoing is exposed to an outside authority with the intention that some kind of action be taken. This action overlaps with the standard definitions of whistleblowing as articulated by Near and Miceli (1985, 1996; see also Miceli et al., 2008) and by Jubb (1999) (despite their differences).

The two examples I will use are (1) three (of the many) U.S. government whistleblower programs: the *False Claims Act qui tam* provisions, the *Securities and Exchange Commission* (SEC) and the *Internal Revenue Service* (IRS), all of which offer financial awards to those who expose government fraud, corporate financial crime, tax evasion and corruption; and (2) citizen 'informing' systems in two Scandinavian welfare states (Denmark and Sweden), where people can report their neighbours to the authorities for cheating on welfare benefits or taxes.

The U.S. Government programs, which can reward whistleblowers with millions of dollars, make it possible for whistleblowers to 'Do good and get rich' (Callahan and Dworkin, 1992). In Denmark and Sweden, informing the local authorities of neighbours abusing welfare benefits is a system of tipstering, variously described as 'civic duty' or 'snitching'. As will be shown, the Scandinavian welfare authorities are ambivalent about offering citizens the ability to inform on their neighbours.

The two examples were chosen not so much because they are new or unique. Rewards (bounties) for informing the government of illegality have a long history, especially in the U.S., with several discussions of both ethical dimensions and the relative costs and benefits (cf. Carson et al., 2007; Dworkin and Brown, 2013; Faunce et al., 2014; Howse and Daniels, 1995). Nor is the ability to tip off the authorities about swindling neighbours; most countries have

some kind of hotline system. What is new, however, are the scale of incentives (potential pay-outs of millions of dollars in the U.S.), the ease with which accusations can be made (with the help of lawyers in the U.S. and/or new technologies in Scandinavia), and the possibility to report anonymously (both U.S. and Scandinavia). In both cases, these disclosure acts reflect people's confrontation with organizational loyalty, a topic much commented upon in the whistleblowing literature (De Maria, 2008; Miceli et al., 1991; Near and Miceli, 1985; Roberts, 2014); and in the Scandinavian case, informing authorities about tax or welfare fraud, while it may be encouraged as civic duty, is also viewed as a breach of community solidarity, social trust, and individual privacy.

These two examples are particularly instructive because they reveal some of the ways in which disclosure regimes can be 'stretched' beyond the particular whistleblower-in-the-firm case. In both cases, disclosure is prodded, reworked and curated, while being attached to regulatory authorities. In the U.S. example, the promise of financial rewards is a clear incentive to obtain and disclose controlled knowledge from the private sector. The whistleblower has not only obtained knowledge; the whistleblower has a commodity to sell. In the Scandinavian example, community solidarity is breached by the rise of social indignation towards others who are viewed as abusing communal resources; 'snitching' becomes the weapon of egalitarian ideology (stealing from the collective) or personal revenge. In both the American and Scandinavian cases, however, disclosure regimes reconfigure social connections and loyalties. Knowledge that escapes invariably means loyalties that dissolve. Let us therefore look more closely at the two cases.

The U.S. whistleblowing regime: Truth, power and money

In the United States, there are no less than 55 federal whistleblower protection laws, and nine federal laws explicitly allowing financial compensation for whistleblowers (summarized in Kohn, 2017; see also www.kkc.com). As both whistleblower attorneys and researchers have noted, whistleblowers are now encouraged more by the incentives for financial compensation than what was formerly 'protection from retaliation' (Dworkin and Brown, 2013; Faunce et al., 2014; Kohn, 2017). U.S. government prosecutors focus on the quality of the information provided rather than the whistleblower's motivation for coming forward. Of the major reward programs, the three most frequently used are the False Claims Act, the SEC Office of the Whistleblower and the IRS Whistleblower Program.

The False Claims Act

The False Claims Act, first enacted in 1863 and revised in 1986, is aimed at firms suspected of defrauding the government, typically through false invoicing of contracts or overpricing (summarized in Carson et al., 2007 and Doyle, 2009). The False Claims Act enables individuals who have knowledge of firms defrauding the government to sue the firms on behalf of the government, known as *qui tam,* and to obtain a portion of the punitive damages. *Qui tam* legal proceedings are not whistleblowing per se, but the cases rely on the kind of insider knowledge that a whistleblower would have, and therefore I include it as part of a disclosure regime. Under the *qui tam* provisions, the Government may choose to join or not join the case, but in either case, the claimant (called the 'relator') can receive up to 25% of the total settlement. In its latest revision, the False Claims Act now allows for treble damages, such that the whistleblower claimant, usually assisted by private legal counsel, can in many cases be awarded several million dollars. Since 1986, 11,980 *qui tam* cases have been litigated, and the U.S. government has recovered 41 billion dollars. Of this amount, the claimants (relators) have been paid 6.5 billion dollars in awards (https://www.justice.gov/opa/press-release/file/1020126/download). In 2017, alone, on the basis of 671 cases, the government obtained 3.7 billion dollars in settlements under the False Claims Act, of which 392 million dollars was paid directly to whistleblowers (U.S. Dept. of Justice, 2017). One of the most well-known *qui tam* cases was that of Tour de France cyclist Floyd Landis, who blew the whistle on his fellow team member, Lance Armstrong, for doping and misrepresentation (Armstrong's team, 'US Postal', was sponsored by a government agency, the postal service). Although Landis himself had confessed to doping and had to repay 800,000 dollars to US Postal, he also received an award of 1.1 million dollars for providing information on Armstrong's false claims to the government (the total settlement was five million dollars) (*The Guardian*, 2018). Some of the False Claim Act settlements are truly spectacular. In one pharmaceutical case, with a 280 million dollar settlement paid by the pharmaceutical company to the government, the whistleblower who brought suit received 78 million dollars (Benzinga, 2017).

With cases like this, little wonder that there are now several major private whistleblower and *qui tam* legal firms advertising to help whistleblowers prepare their cases, for which the firms receive a generous percentage of the settlement. One example is the firm of Kohn, Kohn and Colapinto (KKC) which advertises itself as the 'Nation's Leading Law Firm for Whistleblower Protection'. KKC's website (www.kkc.com) lists dozens of successful settlements, and partner Stephen Kohn has authored the authoritative *The new whistleblower's handbook* (Kohn, 2017), listing all the various laws and *qui tam* provisions (Kohn is also

representing the Danske Bank whistleblower Howard Wilkinson and accompanied Wilkinson when he testified before the Danish parliament in October 2018). KKC is also a major force behind an NGO known as the National Whistleblower Center (www.whistleblowers.org).

The SEC whistleblower program

The *Securities and Exchange Commission* (SEC) office of the Whistleblower program was established in 2010 under the Dodd-Frank Act for Wall Street Reform and Consumer Protection (www.sec.gov/whistleblower). The program focuses on SEC's target group, which are publicly traded companies, stock and bond markets, etc. The SEC program allows whistleblowers to report financial irregularities or corruption to the U.S. Securities and Exchange Commission (which oversees financial transactions and other potential economic crimes). The whistleblower can come forward by name or can report anonymously, in which case they are represented by an attorney. The whistleblower need not be an organizational insider, nor must they be a US citizen.

According to the SEC statistics (U.S. Securities and Exchange Commission, 2018), about one-quarter of whistleblowers report anonymously (and are therefore represented by counsel). If the disclosed knowledge results in a case and a settlement of over one million dollars, the whistleblower becomes eligible for an award of from 10% to 30% of the settlement. Between 2010, when the program began, and 2018, 326 million dollars has been awarded to 59 individuals (this and other data from U.S. Securities and Exchange Commission, 2018). In 2018 alone, 13 individuals received a total of 168 million dollars. Since 2013, the ten largest awards, some of which are shared, have ranged from 8 to 50 million dollars. The largest award to a single individual was 39 million dollars. Higher awards are given if the information provided by the person is significant or if they initially reported the irregularity through their firm's internal reporting channels. The award is lower if the individual was themselves culpable or if they came forward under threat of prosecution.

In total, the SEC whistleblower program has helped the SEC impose 975 million dollars in penalties on firms and individuals, of which 671 million was disgorgement of ill-gotten gains (this and following statistics from U.S. Securities and Exchange Commission, 2018). Since August 2011, the SEC Office of the Whistleblower has received 28,000 tips, with 5282 in FY 2018 alone. The tips, from 114 countries, are classified according to the kind of corporate illegality and the origin of the reporting individual. Of the total whistleblowers in FY 2018, 69% of the recipients were employee insiders, 83% had first raised concerns

internally, 54% were represented by counsel, and of these, 19% filed anonymously.

Besides disbursing cash awards, the SEC program also seeks to protect whistleblowers. The SEC prohibits firms from imposing confidentiality clauses or non-disclosure agreements on employees if the employee believes that the law is being violated. The SEC is thus attempting to restructure the corporate disclosure regime. Moreover, the SEC provides protection from retaliation, not only awarding compensation but also paying for legal assistance.

The IRS Whistleblower Office

The *Internal Revenue Service* (IRS) has a simple mandate: to collect taxes. Its task is therefore to ascertain if there is unreported income (often hidden abroad) or non-payment of taxes. Whistleblowers can contact the IRS Whistleblower Office if they think some person or firm is evading taxes by hiding or misreporting income. Anyone who has ever filed a US tax return (as I have), knows that the IRS has a form for everything. Whistleblowers use IRS Form 3949A, which is an 'Information Referral' form. To claim a financial award, one can fill out form 211, an 'Application for Award for Original Information'. In 2017, 29,000 submissions were sent to the IRS, of which 12,000 were rejected as irrelevant or not credible and the remainder investigated in some form (this and following statistics from Internal Revenue Service, 2017). The IRS Whistleblower Office has a staff of 61 persons. The award amount can range from 15-30% of the assessed penalty or settlement. The IRS does not as yet guarantee whistleblower protection. And since cases may take a long time to resolve, it informs whistleblowers that they can first expect their 'reward' only *five to seven years* after reporting.

Since 2007, the IRS has awarded 465 million dollars to whistleblowers based on the collection of 3.4 billion dollars from tips. In FY 2017 alone, the IRS Whistleblower Office paid out 61 million dollars to 418 persons (Internal Revenue Service, 2017). The most spectacular payment, however, was in 2012, when the IRS paid an award of 104 million dollars to a former bank manager in the Swiss UBS scandal (the manager himself was in prison for fraud at the time) (Kocieniewski, 2012). This individual was represented by Kohn, Kohn and Colapinto, as their website and Kohn's (2017) book reminds us (see also www.kkc.com).

The IRS is aware that informing on tax evasion can be personally complicated. They thus advise potential whistleblowers that:

> The IRS is looking for solid information, not an 'educated guess' or unsupported speculation. We are also looking for a significant Federal tax issue – this is not a program for resolving personal problems or disputes about a business relationship. (Internal Revenue Service, 2018)

Whistleblowing under the *qui tam* False Claims Act litigation, SEC, IRS or other laws is both complicated and often risky; many whistleblowers have themselves been implicated. As a result, there are now a number of whistleblower NGOs and whistleblower attorneys whose task is to help individuals file claims in return for a share of the whistleblower's award. Several of these firms advertise that their staff contains former SEC or Department of Justice prosecutors. The firm Labaton/Sucharow, e.g., with the slogan 'SEC Whistleblower Advocate', offers an elaborate assessment test to see if the prospective whistleblower's information is of the type that could benefit from their services (see https://www.secwhistleblowerадvocate.com/faq/). Another firm, Philips and Cohen, provides an extensive listing of successful cases, explaining the penalties assessed and awards received by their prospective clients (see https://www.phillipsandcohen.com/success-stories/whistleblower-stories/). The Kohn, Kohn and Colapinto site offers a comprehensive listing of federal and state whistleblower protection laws, along with an offer to purchase Steven Kohn's (2017) *The new whistleblower's handbook*.

With dozens of whistleblower attorneys vying to receive a percentage of multi-million dollar awards, the whistleblower has now become a sought after commodity, what more cynical observers have termed a veritable 'bribery racket' (Vardi, 2010a, 2010b). Reward programs such as these, with their millions of dollars in pay-outs split between the ambitious whistleblower and the whistleblower law firm, certainly alter the incentives for disclosure. Speaking truth to power is now a commodity. The possibility of a financial reward and whistleblower protection can now encourage the escape of knowledge from corrupt firms; the attorneys can package this escaped knowledge in order to take a percentage of the reward. The *qui tam* legal option and the U.S. whistleblower reward programs show that there is no contradiction between an individual's motive to expose wrongdoing and seeking a life-changing financial reward. 'Do the right thing' can go along with 'follow the money'.

In summary, the U.S. disclosure regime is characterized by the priority given to a financial reward. Based on knowledge escape within private firms, whistleblowers have options to which their escaping knowledge can be channelled: a *qui tam* trial, or the various government organs where many competencies overlap. Finally, this disclosure regime highlights the role of key intermediaries who can commodify this knowledge into a product by which the 'knower', in this case a corporate whistleblower, can earn a compensation or

become a celebrity. As such, it is a *corporate* disclosure regime in which escaped knowledge has a price tag.

Community whistleblowing in Scandinavia

My second example of a disclosure regime comes from Scandinavia, specifically Denmark and Sweden (where I have lived and worked). The disclosure practice to be described can be termed 'informing', 'tipstering;' 'snitching' or 'community whistleblowing'. It lies at the interface between citizens, neighbours and authorities in countries with high taxes and generous welfare benefits. The units of knowledge are individuals living in communities. As such, it is a disclosure regime in which the informing neighbour is disloyal, but not to an organization. The informer is disloyal to a neighbourhood ethos of 'non-interference in private life', or to a friendship or family unit in which certain affairs are supposed to remain 'between us'. Neighbourhoods, friendship groups and families are not organizations, of course. But they do organize in the sociological sense. People who live in proximity to each other or have social obligations can relate to each other in a matter which is intimate, friendly, neutral or hostile. Families and neighbours organize common activities of work or leisure pursuits, social or material exchanges of goods or favours, or interact through networks of friends and acquaintances. In these relations, certain kinds of knowledge become known, and some of it may escape the inner circle. Here I will describe Scandinavian-style welfare tipstering as a type of disclosure regime, with the intention of showing how it overlaps with whistleblowing in organizations. It is not the intention here to show that tipstering is whistleblowing. Rather, the goal is to show that tipstering and whistleblowing are embedded in different types of disclosure regimes.

All countries encourage citizens to report abuse of state benefits to the authorities. Scandinavian countries distinguish themselves with generous social benefits coupled with the world's highest taxes. Both tax paying and tax evasion are social acts with moral implications. The high level of social trust in Scandinavia, and Scandinavian social cohesion generally, is based on people's perception of whether this elaborate social contract of high taxes-high benefits is being upheld. A perception of injustice – that I am paying my share into the collective while someone else takes undeserved benefits (welfare cheating/undeclared income/tax evasion) – will lead to indignation. The indignation can be sparked by observations of a neighbour, acquaintance or family member with unexplained wealth, or by a scandal exposed in the media. Popular indignation, fanned by periodic welfare or tax cheating scandals, fuels a variety of responses: administrative reforms by the government, more

surveillance of clients, populist movements against too much surveillance, or legitimizing one's own tax cheating as a justified form of social revolt ('everyone is doing it'). Much of the indignation against immigrants and refugees in the Scandinavian countries, for example, is founded not so much on nationalism or racism, but on the sentiment that especially newly arrived immigrant groups are preying on the welfare state, for example, by not working, receiving too many welfare benefits (housing, child payments) or by not paying their fair share of taxes.

It is at this threshold of indignation that individuals can decide to blow the whistle on neighbours, ex-spouses or acquaintances whom they believe are cheating the system. This threshold is transcended when trust between community members declines or is breached. Typically, the social bonds of neighbourliness, bonds formerly forged by shared experiences of class, workplace, ethnic bonds, public school attendance and community associations, begin to weaken. Alienation from each other, neighbours whom you do not know or trust, leads to people becoming willing to inform authorities about illicit behaviour of neighbours, acquaintances or estranged family members. The ability to do this by clicking your iPhone makes it that much easier.

Scandinavian welfare states dole out generous benefits (welfare) but demand citizen contributions (taxes). In the Scandinavian welfare systems, undue benefits can take the form of failure to declare cash income or assets while receiving welfare or unemployment payments, misrepresenting one's personal situation (single parents who are in reality co-habiting), faking sickness or disability in order to receive a pension, and various home health care scams with false caretaker receipts. In the tax area, the illicit practices could include undeclared income (typically extra work or income in construction, catering and household services) or working while receiving welfare benefits. Both types of abuses – welfare cheating and tax fraud – reflect a mismatch between the information that individuals must provide to the authorities (change in life circumstances, reported extra income) and how the authorities then calculate welfare payments or tax obligations. In all the Scandinavian countries, these two kinds of deception are the constant topic of press commentary, political rhetoric, and bureaucratic control measures. For example, in Denmark, welfare authorities can check recipients' bank accounts for sudden withdrawals of cash by a client seeking to show that they have no assets. They can check single mothers' Facebook pages to see if they are co-habiting (Gaardmand, 2011; Madsen and Frederiksen, 2017). Welfare authorities are also stationed at airports to stop returning vacationers and determine whether they have been receiving unemployment benefits while abroad, which violates their promise to be 'available to the labour market' (Kristensen, 2018). The welfare system 'sends

signals' (their expression) to potential cheaters that 'We are everywhere', and 'It doesn't pay to cheat'.

In the last decade, public authorities have made explicit appeals to citizens to submit information about suspected cheaters in their communities. The result is the rise of what Danish officials have called the 'cheat button' (*snydknappen*), also called 'gossip service' (*sladretjeneste*) or 'snitch line' (*stikkerlinie*). The integration of citizens, community groups, firms or private security companies in enforcing the law (called 'plural policing', cf. O'Neill and Fyfe, 2017) is a trend in many arenas of public life, and this includes welfare cheating. Some media commentators and politicians have termed this tendency to be the onset of an 'informer culture'. The Danish and Swedish words used (*stikker, angivar, meddelare*) are similar to words used about wartime snitches during the Nazi occupation of Denmark. The Danish rhetoric about this kind of practice talks of a 'collaborator society', 'informer society', 'surveillance society', even 'Stasi society', or 'Stasification' (*stasificering*) (Larsen, 2010). In Sweden (which had no Nazi occupation) the rhetoric is also of an 'informer society', but here the reference is to Eastern European secret police (Jensen, 2013).

Disclosure pressures in Scandinavia have been intensified as a result of horrific cases of child abuse in outlying communities that went unreported or were overlooked by the authorities. The issue was whether neighbours should have intervened earlier. The imperative to interfere in cases of suspected child abuse runs up against ingrained traditions not to intrude on a neighbour's private life. Scandinavian citizens are constantly being asked to 'get involved' on the one hand, but to 'be careful about interfering in people's private lives' on the other. Apparently, we should interfere if there is abuse, but perhaps live and let live if it is a neighbour working off the books or receiving undeserved welfare benefits. The cheating neighbour is not mistreating a child, but they are violating some kind of social trust. And it is here that welfare cheating or tax evasion may be the subject of disclosure, with the expectation that 'something will be done'. What we have here is the familiar model of whistleblowing articulated in works by Near and Miceli (1985, 1996), Miceli et al., (2008) and Lewis et al., (2014), with its various phases (discovery of an abuse, weighing decision to report, reporting to internal and then external authorities, awaiting action, etc.) and cast of characters: the guilty party, the whistleblower, the organization, the external authority, the public, the media. There are thus clear parallels between the corporate whistleblower and the neighbourhood snitch across the street.

While Scandinavian citizens, like those elsewhere, have always been able to report tax cheating or welfare abuse by their neighbours, new initiatives by local municipalities and the ease of digital solutions have led to the establishment of

fraud reporting web portals. Where there used to be telephone hotlines and letters, indignant citizens can now easily click their way to an accusation of tax or welfare swindle. They can make an accusatory report and even upload 'evidence' in the form of surveillance photos taken with their cell phone, literally across the fence or from their window (see Borger.dk, 2018 (www.borger.dk/anmeldesnyd); Skatteverket 2018 (www.skatteverket.se/Tipsa om misstänkt fusk)). No monetary rewards are given for this citizen vigilance. The informer's reward is purely intrinsic. It is a feeling of social justice, a release of pent-up indignation, or downright revenge against a neighbour, ex-spouse or former business partner whom they feel is getting more than they deserve. Let me therefore provide some details of the informing landscape in Denmark and Sweden.

Denmark: Informing as community whistleblowing

In Denmark, 20% of the population is estimated to know someone who has swindled the welfare payments system, and approximately 10% of benefits are paid out on the basis of swindle (KMD Analyse, 2011). Presently, all of Denmark's 98 municipalities have web sites where people can report abuse or false welfare claims, typically for public assistance, single parent child allowances or disability (not all of them have anonymous reporting options, however). Abuses of the system can consist of undeclared income ('black work') or a pro-forma divorce where one spouse has an official address elsewhere but in fact lives in the home (a Danish single parent receives a 'single-parent' benefit and reductions in day-care fees). Citizen informants can submit photo evidence by name and in some municipalities anonymously.

The Danish municipalities have 'control units', which assess welfare entitlements and can demand restitution of illicitly received benefits (Madsen, 2013). In 2017, these units investigated handled 20,349 cases of suspected abuse (Kommunernes Landsforening, 2018). Of these 429 (2%) came from named individual accusers, and 2882 (14%) from anonymous sources (the remainder came from other public authorities); these reports resulted in restitution of 6.2 million DKK in illegally received welfare benefits to the municipalities and an additional savings of 26.1 million DKK that would have been subsequently dispersed improperly in the future (*ibid.*). However, fully 83% of the anonymous accusations and 84% of the named accusations either lacked proper information or were judged incorrect or too trivial to pursue. Danish municipalities now exchange more information with other agencies using various national registers, a coordination effort which has led to more cases of abuse being discovered and resolved without the use of informants.

In addition to the municipal welfare offices, the national Danish tax authorities have also set up a reporting site for suspected tax swindle. Reports from citizens, firms and authorities numbered 6878 in 2011, rising to 10,541 in 2013. Sixty percent of these reports are anonymous (Berlingske, 2013). The accusations involved violations such as untaxed income or hiring illegal workers (who were usually paid in cash, hence unreported income). According to one tax official, of 6800 citizen complaints received in 2012, one-third were 'not serious' or simple harassment of a neighbour (Schultz, 2012). The tax ministry's surveys say that citizens' acceptance of undeclared income ('black work') is declining, which has led to an increase in the number of reports. According to the tax official, 'We have a veritable informer culture out in the suburbs' (*ibid.*). Yet some politicians have misgivings. The minister of taxation, from the left-wing Socialist People's party, declared, 'We should avoid the Ministry of Taxation being used in a feud between family members or neighbours' (Ritzau, 2013). The minister was not far off, as a 2008 report found that one-third of all citizen tips to the Danish tax authorities derived from family conflicts, ex-spouses, or cheated customers (Politiken, 2008). The use of the 'cheat button' was criticized by several commentators as a step toward a Stasi-like society (Borre-Jensen, 2012; Jensen, 2010; TV2, 2012), or even a 'Stasification' of Denmark (Engel-Schmidt, 2012). The nanny state is being replaced by the Stasi state, or as one commentator put it, 'from Big Mother to Big Brother' (Jensen, 2010). Subject to these pressures, and with a change to a conservative government, the newly appointed minister for taxation decided to close the anonymous web portal, saying that it could be abused (Larsen, 2015). Some Danish political parties take offense at the informer society: an MP from a left-wing party, for example, declares that 'the authorities should realize that even though someone perhaps receives a payment that they are not allowed to, it cannot legitimate a surveillance society where we run around and take pictures of each other' (Lauridsen and Quass, 2013). In Copenhagen municipality, which has a majority left-wing administration, the anonymous reporting option was closed down in March 2019 (the center and right parties were opposed). One of the politicians criticizing the 'snitch society', declared, 'I am against the mistrust that [the cheat button] creates when it encourages us to inform' (Grünfeld, 2018). Disclosure regimes clearly create their own anxieties revolving around trust.

Informing in Sweden

In Sweden, informers can send information about abuse to several sites: the tax ministry, the state social insurance payment agency (Försäkringskassan/FK), or to other bureaus such as the Immigrant and Migration Agency. Typical welfare crimes, covering both false claims and abuse of payments, include falsifying disability, sick leave, student stipends, housing stipends and payment for caring

for the disabled or sick children (VAB). The Swedish tax ministry receives about 20,000 tips per year via letter, phone, email and other channels. The tips to the tax ministry were primarily concerned with off-the-books work, especially in construction, hairdressing and café/restaurant.

The Swedish social insurance payment agency (Försäkringskassan/FK), received 16,771 cases of suspected abuse referred from all sources (other authorities, the public) in 2015, up from 4000 in 2005 and 9653 in 2009 (Försäkringskassan, 2016). Of these 16,771 cases, 7395 (43%) came from the public (*ibid.*). However, only 17% of these citizen tips resulted in any follow-up measures, such as demand for payment or criminal charges (*ibid.*). The implication here is that the vast majority of the reports submitted by individuals, as in Denmark, are less useful to the authorities or less reliable. As a Swedish official explained, the anonymous reports 'are often more about frustration than they are substantive, and in most of the cases, the person [being accused] has the right to receive payment' (Haglund, 2013). The head of the tax authority adds a note of caution:

> It's a bit sensitive. We don't want to have an informer society where you create insecurity. It feels wrong, without me being able to say exactly why. Wouldn't you yourself feel that it was sleazy? There are often conflicts and family tragedies behind the tips. We don't want to dive in and punish and make life difficult for the person. (Faktum, 2010)

Consequences of the Scandinavian disclosure regime

The propensity for people to inform is a much discussed, but little researched topic in Sweden. A Swedish net-based survey of 43,000 persons conducted in 2010 (by the newspaper *Aftonbladet*) found that 35% of respondents would report their neighbours for welfare cheating, 26% said they would not, but 33% said, 'it depends on the neighbour' (Faktum, 2010). Apparently, the quality of neighbourly relations is as important for whistleblowing as any notion of higher civic duty. Community whistleblowing in Scandinavia seems dependent on a situational morality: 'It depends on the neighbour'.

Summarizing, both Danish and Swedish public authorities are aware that encouraging informing may threaten their highly touted social cohesion and general level of social trust. A Swedish official cautions: 'We do not work "actively" to get tips in from the public' (Haglund, 2013). He does not encourage an 'informer culture' (*angivarkultur*). 'We do not have major publicity campaigns [encouraging people to] call us if you think there is swindle going on' (*ibid.*). Another official acknowledges the many motives for informing on neighbours 'We know that it can be about gossip, revenge, and there can be other interests which are served by the information' (Faktum, 2010).

One of the more problematic aspects of the reporting culture is the stigmatization of those who are socially vulnerable. The head of the Swedish association of disabled persons, for example, complained that the media and the authorities create the impression that it is easy to swindle, and that people do not know how many assessments that disabled people must undergo in order to obtain their disability pensions (Sveriges Radio, 2013).

In sum, systems where general trust is under pressure can create conditions for conflict, and one channel for this kind of conflict is the use of an informant culture where people disclose secrets about their neighbours, ex-spouses or former business partners. Whether we want to call this 'whistleblowing' is an academic issue. It is certainly disclosure, in so far as it is knowledge that escapes. And it has broader implications for how people in Scandinavian states interact with each other, and with the authorities to whom they pay taxes and from whom they receive welfare benefits.

Conclusions: Regimes, rewards and revenge

The notion of disclosure regimes is a way of talking about how knowledge is controlled, constrained, dispensed and escapes. Some of this escaping knowledge is trivial or short-lived, or at best scandalous. But some escaping knowledge can alter the knowledge landscape, releasing new forms of emancipation or ever more regulation. If organizations, as well as other social groups, are composed of knowers, then we need to follow their strategies and practices. This means understanding who seeks to control and constrain what kinds of knowledge, and who may possibly decide to steal it, leak it, or allow this knowledge to escape. Social cohesion, organizational loyalty and community trust all play into these processes of knowledge control. Whistleblowing in corporate America, and informer snitching in Scandinavian neighbourhoods, are ways in which escaping knowledge reveals changing social constellations of trust and distrust.

Whistleblowing has up to now been seen as a practice confined to organizations. Theorists have offered us descriptions, typologies, phases, actors, and effects of this process. Yet the pressure toward transparency, toward disclosure, toward making the private public in the hope of redressing an injustice or obtaining a reward is not simply a property of formal organizations. It is a property of all social groups. We thus need to view organizational whistleblowing as one moment on a continuum of knowledge escape that would include personal confessions, revelations of abusive behaviour committed by authorities or employers, as a means of individual empowerment against organizations, as an expression of employees' ethical opposition to their organizations' wrongdoing,

as a political tool used by the leaker who downloads to WikiLeaks, as a means of making money, and finally, as a form of social conflict among envious neighbours and community members. Each of these disclosure practices contains forms of empowerment, in which individuals take, or *take back*, some kind of control over their life circumstances. Their actions may not necessarily derive from the most noble of motives. After all, social life operates through this very mixture of higher moral/civic duty and a personal project (e.g., making a few million dollars, getting even with an ex-employer or with a nasty neighbour). Disclosure practices can thus combine civic duty with personal agendas. Such combinations are neither strange nor deviant. They are the stuff of social life.

Whistleblowing in the United States has now become a matter of knowledge for sale. The government whistleblowing rewards programs can help bridge the gap between the individual disloyalty and their organization's secrets. The government recognizes and apparently encourages this breach by paying higher rewards to those who have gone through organizational channels first.

In Denmark and Sweden, meanwhile, the community informing articulated as civic duty provides a cover for ordinary neighbourly envy and perhaps revenge under a civic duty to report. Some time ago, local and neighbourly loyalties took precedence over the prying eyes of the state. People were left alone, even though there was the risk of domestic violence or child abuse. No more. Being a good citizen means identifying and reporting cheating neighbours. This practice may be criticized as a Stasi-like surveillance, but this would be an oversimplification. However, like the communist informer systems, the Scandinavian disclosure regime allows people to use the state as a vehicle for personal 'getting even'. It is not Stasi surveillance, but it is a form of everyday totalitarianism and iPhone surveillance.

These Danish and Swedish debates over citizen informing take place in high trust societies. People believe, and expect, that 'the system' can solve their personal problems and should treat people fairly and equitably. This raises several questions: To what degree is citizen reporting on neighbours or acquaintances an indication of civic duty or of a more mundane type of personal envy and indignation? To what extent is the Scandinavian neighbourhood disclosure regime a litmus test of society's social cohesion? How do we gauge whether it is better for neighbours to be suspicious and interfere, or whether, in the name of community harmony, to just leave their fellow neighbours alone as they 'play' the system for what they can get? If citizens are expected to 'become involved' in cases of suspected child abuse, then why not interfere when you see welfare cheating or untaxed income? One might argue, of course, that the child is an innocent victim who may be brutally harmed, while welfare cheating is

'victimless'. But wait, there is a victim. It is, well, *us*, society. So there is perhaps an ethical prescription to inform on the neighbour's illicit practices. Someone is being harmed: us. The nosy Danish or Swedish neighbour pressing the 'cheat button' or sending pictures from her iPhone may be acting out of personal envy or revenge, but it is now channelled as a civic duty. Perhaps it is this combination of the large and small projects – civic duty mixed with personal indignation – that comes together in the Scandinavian welfare disclosure regime. It is both big and small; civic and petty. Tipping off the authorities, clicking the 'cheat button', is a way in which the powerless tell the powerful *about other powerless*. Unlike in the U.S., where the motivation to inform is subordinate and information can be paid in cash, the Scandinavian authorities offer no rewards to snitches. Moreover, authorities insist on describing their initiatives as the opposite of any kind of 'informer culture' and are certainly ambivalent about the use of anonymous accusations. The authorities know that such informing, while it may be justified by a civic duty, can also be driven by envy or jealousy over a neighbour suspected of misusing public goods, receiving undue benefits, or evading taxes). The authorities operate from some kind of disclosure regime denial, while encouraging disclosure as vendetta egalitarianism. This is truly the dark side of the disclosure regime.

Getting paid to expose corporate wrongdoing and uploading photos of a supposedly disabled neighbour jumping on their backyard trampoline may seem quite different from each other. But I believe that they are both examples of the kinds of disclosure regimes in which we dwell. It is transparency combined with vengeance at the popular level. Our understanding of organizational whistleblowing thus needs to be broadened. We need to see organizational whistleblowing as part of more inclusive broader regimes of disclosure and agendas of transparency. Organizational researchers certainly understand that organizations exist within society. In this same sense, whistleblowing in organizations should be seen as part of a larger dynamic of disclosure, with common motivations, incentives, constraints and consequences. Hence, we need to study *who tells what about whom to whom*. We need to study how they tell it and what happens to the truth-teller/accuser and the accused after the disclosure act. Most importantly, we need to understand that disclosure regimes will invariably involve a mixture of high-minded goals and personal motivations; they will also spawn new kinds of regulatory frameworks pushing 'whistleblower protection' on one hand but 'more transparency' on the other. We thus need to better understand the kinds of incentives, motivations, and structural constraints that stimulate, sustain or threaten regimes of disclosure. And we need to see disclosure not solely as a matter of individual persons who either tell or keep secrets, but as social systems where conditions can stimulate, constrain or manage the way knowledge is created and how it escapes. Disclosure is a social

act. Finally, let us remember that most people are not whistleblowers. Most people choose to keep silent about abuses in their organizations and among their neighbours. At least until they themselves are implicated, hacked, or threatened by jail. Employees or neighbours who keep secrets may be doing so because of intimidation, or fear of expulsion, or because of a genuine loyalty to their superiors, their firm or their community, combined with a resistance to prying authorities. In this latter sense, not to inform on others is a political act, an act of solidarity. Knowledge control and disclosure are thus processes that take place between people. They are social processes.

Whether it be U.S. government whistleblower schemes or community informing in Scandinavia, acts of disclosure highlight the relationship between individuals and their organizations, between the ambiguity of belonging and the tensions inherent in organizing. The call to the whistleblower attorney promising a million dollar pay-out, or the uploading of some photos and a few anonymous clicks on the 'cheat button', may make the disclosure process easier at the outset, but this does not resolve the inherent tensions between individuals and the organizing milieus in which we live. Social life – be it in organizations or communities – is full of these tensions, and much of the tension revolves around managing knowledge. Disclosure regimes confront the basic knowledge management issue as it applies to all social groups: Who should know what about us? Whistleblowing and informing amplify the conflict between regimes of disclosure, imperatives for transparency, the everyday life of organizations and communities and the secrets that hold them together. Within a broader context of disclosure regimes, acts of personal confession, revelations of abuse, informing on neighbours and leaking sensitive information, whistleblowing about corruption and other forms of public exposure and disclosure lay bare the tense relation between workers and employers, citizens and the state, and between neighbours and each other. It is customary to celebrate transparency and whistleblowing. Don't be too sure. Disclosure regimes have a dark side that we are only now beginning to see.

references

Barth, F. (2002) 'An anthropology of knowledge', *Current Anthropology,* 43(1): 1-17.

Benzinga (2017) 'Whistleblower receives $78 million relator share in False Claims Act suit against pharmaceutical giant Celgene', 12 December. [https://www.benzinga.com/pressreleases/17/12/p10949803/whistleblower-receives-78-million-relator-share-in-false-claims-act-su]

Berlingske Tidende (2013) 'Danskerne angiver hinanden som aldrig før', 20 October. [https://www.berlingske.dk/samfund/danskerne-angiver-hinanden-som-aldrig-foer]

Birchall, C. (2011) 'Introduction to "secrecy and transparency": the politics of opacity and openness', *Theory, Culture and Society,* 29: 7-25.

Borger.dk (2018) 'Anmeld mistanke om snyd'. [https://www.borger.dk/oekonomi-skat-su/Kontrol-sociale-ydelser-oversigt/Kontrol-sociale-ydelser-anmeld]

Borre-Jensen, R. (2012) 'Anmelderi fører til Stasi-samfund', TV2 nord.dk 28 October. [https://www.tv2nord.dk/artikel/anmelderi-forer-til-stasi-samfund]

Callahan, E.S. and T.M. Dworkin (1992) 'Do good and get rich: financial incentives for whistleblowing and the False Claims Act', *Villanova Law Review,* 37: 273-336.

Carson, T., M.E. Verdu and R. Wokutch (2007) 'Whistleblowing for profit: an ethical analysis of the federal False Claims Act', *Journal of Business Ethics,* 77(3): 361-376.

De Maria, W. (2008) 'Whistleblowers and organizational protesters: crossing imaginary borders', *Current Sociology,* 56 (6): 865-883.

Doyle, C. (2009) *Qui Tam: The False Claims Act and related federal statutes.* Washington: Library of Congress. Congressional Research Service.

Dworkin, T.M. and E.S. Callahan (1998) 'Internal vs. external whistleblowers: a comparison of whistleblowing processes', *Journal of Business Ethics,* 17(12): 1281-1298.

Engel-Schmidt, J. (2012) 'Kommunen mangler penge – stik din nabo', *Politiken,* 3 July. [https://politiken.dk/debat/profiler/engel-schmidt/art5396716/Kommunen-mangler-penge-stik-din-nabo]

Faktum (2010) 'Gör en insats – ange din granne', 24 November. [https://www.faktum.se/gor-en-insats-ange-din-granne/]

Faunce, T., K. Crow, T. Nicolic and F.M. Morgan (2014) 'Because they have evidence: globalizing financial incentives for corporate fraud whistleblowers', in A.J. Brown, D. Lewis, R. Moberly and W. Vandekerckhove (eds.) *International handbook on whistleblowing research*. Cheltenham, UK: Edward Elgar.

Flyverbom, M. (2016) 'Disclosing and concealing; internet governance, information control and the management of visibility', *Internet Policy Review,* 5(3): 1-11.

Flyverbom, M. and O. B. Albu (2017) 'Transparency', in C. R. Scott and L. Lewis (eds.) *The International encyclopedia of organizational communication*. West Sussex: Wiley Blackwell.

Försäkringskassan (2016) 'Särskild redovisning av felaktiga utbetalningar', 19 February. [https://assistanskoll.se/_up/regeringsuppdrag_felaktiga_utbetalningar.pdf]

Gaarmand, N.G. (2011) 'Enlig mor overvåget ulovligt i over et år', *Dagbladet Information,* 21 March. [https://www.information.dk/indland/2011/03/enlig-mor-overvaaget-ulovligt-aar]

Gladwell, M. (2016) 'Daniel Ellsberg, Edward Snowden, and the Modern Whistleblower', *The New Yorker,* 11 December. [https://www.newyorker.com/magazine/2016/12/19/daniel-ellsberg-edward-snowden-and-the-modern-whistleblower]

The Guardian (2018) 'Lance Armstrong reaches $5m settlement in $100m federal fraud case', 19 April. [https://www.theguardian.com/sport/2018/apr/19/lance-armstrong-settlement-usps-lawsuit]

Grünfeld, N. (2018) 'Vi skal ikke gå rundt og stikke hinanden', *BT*. 21 August. [https://www.bt.dk/debat/vi-skal-ikke-gaa-rundt-og-stikke-hinanden]

Haglund, A. (2013) 'Grannar hjälper FK avslöja fuskare', *Dagens Nyheter,* 10 November. [https://www.dn.se/nyheter/sverige/grannar-hjalper-fk-avsloja-fuskare].

Han, B.C. (2015) *The transparency society*. Stanford, Ca: Stanford Brief.

Heemsbergen, L. (2016) 'From radical transparency to radical disclosure: reconfiguring (in) voluntary transparency through the management of visibilities', *International Journal of Communication,* 10: 138-151.

Howse, R. and R. Daniels (1995) 'Rewarding whistleblowers: the costs and benefits of an incentive-based compliance strategy'. University of Pennsylvania School of Law, Departmental Papers Series. [http://://repository.upenn.edu/law_series/4]

Internal Revenue Service (2018) 'Whistleblower informant award'. [https://www.irs.gov/compliance/whistleblower-informant-award]

Internal Revenue Service (2017) 'IRS Whistleblower Program. Fiscal Year 2017 Annual Report to Congress'. [https://www.irs.gov/compliance/whistleblower-office-annual-reports]

Jensen, T. (2010) 'Danskerne som stikkere – Big Mother og Big Brother II', *Berlingske Tidende* 13 November. [https://tomjensen.blogs.berlingske.dk/2010/11/13/danskerne-som-stikkere-big-mother-og-big-brother-ii/]

Jensen, T. (2013) 'Stikker du?', *Berlingske Tidende*. 7 August. [https://tomjensen.blogs.berlingske.dk/2013/08/07/stikker-du/]

Jubb, P. (1999) 'Whistleblowing: A restrictive definition and interpretation', *Journal of Business Ethics,* 21: 77-94.

KMD Analyse (2011) 'Socialt bedrageri i Danmark: Omfang, adfærd og holdninger.'
[http://://publikationer.kmd.dk/Analyser/Socialtbedrageri_i_Danmark/#/]

Kocieniewski, D.(2012) 'Whistleblower awarded 104 million by IRS' . *The New York Times*, 12 September. [https://www.nytimes.com/2012/09/12/business/whistle-blower-awarded-104-million-by-irs.html]

Kohn, S. M. (2017) *The new whistleblower's handbook: A step-by-step guide to doing what's right and protecting yourself*. Guilford, Connecticut: National Book Network.

Kommunernes Landsforening (2018) 'Effektmåling 1. Halvår 2018'.
[https://www.kl.dk/media/16943/kl01s109-priv-kali-personal-user-shell-folders-desktop-effektmaaling-af-kommunernes-kontrolindsats-1-halvaar-2018.pdf]

Kristensen, V. (2018) 'Kontrol i lufthavnen afslørede socialt bedrageri for 10,6 millioner', *Avisen.dk*, 13 March. [https://www.avisen.dk/top-fem-aars-lufthavnstilsyn-afsloerede-blot-106-mio_489430.aspx]

Lampert, N. (1988) *Whistleblowing in the Soviet Union: complaints and abuses under state socialism*. London: MacMillan.

Larsen, L. K. (2015) 'Skatteminister afskaffer anonym anmelde tjeneste', Danmarks Radio, 1 September. [https://www.dr.dk/ligetil/indland/skatteminister-afskaffer-anonym-anmelde-tjeneste]

Larsen, R. E. (2010) 'Danske Stasi-tendenser og retsløs klapjagt på ledige', *Politiken,* 11 October. [https://politiken.dk/debat/arkiv_debattoerer/engelbreth/art5046287/Danske-Stasi-tendenser-og-retsl%C3%B8s-klapjagt-p%C3%A5-ledige]

Lauridsen, J. and L. Quass (2013) 'Enhedslisten harmes over opfordring til angiveri', *Jydske Vestkysten,* 11 July.
[https://jv.dk/artikel/enhedslisten-harmes-over-opfordring-til-angiveri-2013-7-11(3)]

Lewis, D., A.J. Brown and R. Moberly (2014) 'Whistleblowing: its importance and the state of research', in A.J. Brown, D. Lewis, R. Moberly and W. Vandekerckhove (eds.), *International handbook on whistleblowing research*. Cheltenham, UK: Edward Elgar.

Madsen, L. B. (2013) 'Socialt bedrageri: En empirisk undersøgelse af mødet mellem borgeren og den kommunale kontrolindsats.' Master's Thesis, School of Social Work, Aalborg University. [https://projekter.aau.dk/projekter/da/studentthesis/socialt-bedrageri--en-empirisk-undersoegelse-af-moedet-mellem-borgeren-og-den-kommunale-kontrolindsats(ae1920b9-287e-4f6f-88fd-7a2db24a09d8).html]

Madsen, L. B: and M. Frederiksen (2017) 'Og hvis vi så ikke må – jamen hvordan skulle vi vide det? Kommunalt kontrolarbejde med socialt bedrageri', *Dansk Sociologi,* 28(1):1-30.

Miceli, M.P., J.P. Near and C.R. Schwenk, C.R. (1991) 'Who blows the whistle and why', *Industrial and Labour Relations Review,* 45(1): 113-130.

Miceli, M., J.P. Near and T.M. Dworkin (2008) *Whistleblowing in organizations.* New York: Routledge.

Near, J.P. and M.P. Miceli (1985) 'Organizational dissidence: the case of whistleblowing', *Journal of Business Ethics,* 4: 1-16.

Near, J.P. and M.P. Miceli (1996) 'Whistleblowing: myth and reality', *Journal of Management* 22(3): 507-526.

Olesen, T. (2019) 'The politics of whistleblowing in digitalized societies', *Politics and Society* 47(2): 277-297.

O'Neill, M. and N. Fyfe (2017) 'Plural policing in Europe: relationships and governance in contemporary security systems', *Policing and Society,* 27(1): 1-5.

Politiken (2008) 'Hver tredje anmeldelse til Skat skyldes hævn', 23 April. [https://politiken.dk/indland/art4741656/Hver-tredje-anmeldelse-til-Skat-skyldes-h%C3%A6vn]

Ritzau News Bureau (2013) 'Anonyme anmeldelser om skattesnyd stiger markant', 21 December. [https://www.fyens.dk/article/2427220:Business-Fyn--Anonyme-anmeldelser-om-skattesnyd-stiger-markant?rss]

Roberts, P. (2014) 'Motivations for whistleblowing: personal, private and public interests', in A.J. Brown, D. Lewis, R. Moberly and W. Vandekerckhove (eds.) *International handbook on whistleblowing research.* Cheltenham, UK: Edward Elgar.

Sampson, S. (2019) 'The morality of transparency: clarity versus emptiness', in F. Osrecki and V. August (eds.) *Der Transparenz-Imperativ. Normen, Strukturen, Praktiken.* Wiesbaden: VS Verlag für Sozialwissenschaften.

Schultz, Nikolaj (2012) 'Flere anmelder sort arbejde', *Danmarks Radio,* 5 March. [https://www.dr.dk/ligetil/indland/flere-anmelder-sort-arbejde]

Skatteverket (2018) 'Kontakt os'. [https://www.skatteverket.se/omoss/kontaktaoss/mejla/tipsaommisstanktfusk.4.7afdf8a313d3421e9a9561.html]

Sveriges Radio (2013) 'Tips om bidragsfusk populart men problematiskt', 22 March. [https://sverigesradio.se/sida/artikel.aspx?programid=3993&artikel=5482818]

Tsoukas, H. (1997) 'The tyranny of light', *Futures,* 29(9): 827-843.

TV2 (2012) 'Ekspert: Anmelderi kan føre til stasisamfund', 2 July. [http:///nyheder.tv2.dk/article.php/id-51513826%3Aekspert-anmelderi-kan-f%25C3%25B8re-til-stasisamfund.html]

U.S. Department of Justice (2017) 'Justice Department Recovers Over $3.7 Billion From False Claims Act Cases in Fiscal Year 2017', December 21. [https://www.justice.gov/opa/pr/justice-department-recovers-over-37-billion-false-claims-act-cases-fiscal-year-2017]

U.S. Securities and Exchange Commission (2018) 'Whistleblower Program, 2018. Annual Report to Congress', November 14. [https://www.sec.gov/files/sec-2018-annual-report-whistleblower-program.pdf]

Vandekerckhove, W. (2006) *Whistleblowing and organizational social responsibility: A global assessment*. Hampshire: Ashgate Publishing, Ltd.

Vardi, N. (2010a) 'The bribery racket', *Forbes,* 7 June. [https://www.forbes.com/global/2010/0607/companies-payoffs-washington-extortion-mendelsohn-bribery-racket.html#331d0571b5a6]

Vardi, N. (2010b) 'The anti-bribery complex', *Forbes*, 7 June. [https://www.forbes.com/forbes/2010/0524/business-weatherford-kbr-anti-bribery-complex.html#2120c7633a0d]

the author

Steven Sampson is Professor em. of Social Anthropology at Lund University. He studies NGOs, anti-corruption and business ethics. Recent publications include 'The "right way": Moral capitalism and the emergence of the corporate ethics and compliance officer' (Journal of Business Anthropology, 2016), 'The anticorruption package' (*ephemera*, 2015), 'Cultures of doing good: Anthropologists and NGOs' (University of Alabama Press, 2017), 'The morality of transparency. Clarity versus Emptiness' (VS Verlag, 2019), and 'Anti-corruption: Who Cares?' (Palgrave, 2019).
Email: steven.sampson@soc.lu.se