TSAS
canadian network for research on
terrorism, security and society

Working Paper Series

No. 17-04

October 2017

'Reporting Suspicion in Canada Insights from the fight against money laundering and terrorist financing'

Anthony Amicelle, School of Criminology, Université de Montréal;

Vanessa Iafolla, Department of Sociology and Legal Studies, University of Waterloo

The Canadian Network for Research on Terrorism, Security, and Society TSAS is supported as a national strategic initiative funded by SSHRC and Public Safety Canada, along with the following departments of the federal government:

- Royal Canadian Mounted Police
- Canadian Security Intelligence Service
- Immigration, Refugees, and Citizenship Canada
- Correctional Services Canada
- Defence Research and Development Canada
- Global Affairs Canada
- Security Intelligence Review Committee
- Office of the Communications Security Establishment Commissioner

TSAS also receives financial support from several Canadian universities, including the University of Waterloo.

Views expressed in this manuscript are those of the author(s) alone.
For more information, contact the Lorne Dawson, Department of Sociology and Legal Studies, University of Waterloo (ldawson@uwaterloo.ca).

Report Submitted to the Canadian Network for Research on Terrorism, Security and Society

Address correspondence to
Dr. Anthony Amicelle, **Assistant Professor in** School of Criminiology
and International Centre for Compartative Criminology, Université de Montréal.
anthony.amicelle@umontreal.ca

Reporting Suspicion in Canada
Insights from the fight against money laundering and terrorist financing

INTRODUCTION

In this new world of catastrophic imagination and uncertainty, there is a shift from the 'culture of control' to a culture of suspicion. (Ericson, 2007: 214)

Has suspicion become the new 'episteme' of our time as a dominant system of thought and perception of social reality for governing (in)security? Although this question is never formulated in an explicit manner, it seems to act as the fuel in criminology, security and surveillance studies. It is especially true within the wide range of academic research and scientific controversies on the current impacts of counterterrorism policing. This body of work is characterized by a shared reference to the semantic field covered by the word 'suspicion', including expressions such as culture of suspicion, atmosphere of suspicion, climate of suspicion, paradigm of suspicion, new age of suspicion, logic of suspicion, net of suspicion, field of suspicion, political economy of suspicion, state suspicion, generalized suspicion, process of suspectification, categorical suspicion and suspect community to name just a few (Shamir, 2005; Amoore and De Goede, 2008; Vaughan-Williams, 2008; Bigo and Guittet, 2011; Hickman et al., 2012; Murakami Wood, 2012; Patel 2012; Bauman et al., 2014; Mythen and Walklate, 2016; Ragazzi, 2016; Guittet and Brion, 2017).

The multifaceted issue of suspicion is mainly addressed in its relation to different but overlapping forms of surveillance (Andrejevic, 2006; Pantazis and Pemberton, 2009; Monahan, 2010). David Lyon sums up the dynamic relationship between surveillance and suspicion in his book Surveillance after September 11 in which "a central theme is the culture of suspicion and how it produces and is produced by surveillance" (2003: 10). Suspicion is approached as both a key driver and a critical result of surveillance practices while surveillance is presented as both a key technique in assembling suspicion and a critical manifestation of suspicion and mistrust (Taylor 2012; Huysmans 2014). To put it bluntly, "surveillance fosters suspicion and suspicion in return supports the logic of maximisation of surveillance" (Guittet, 2015: 2).

The increasing importance of 'suspicious activity reporting' is certainly the most glaring example of such an extensive and mutually supportive articulation between surveillance and suspicion for law-enforcement and counterterrorism purposes. In this respect, much has already been written about the renewed emphasis on public campaigns urging citizens and businesses to contribute to national security intelligence (Chan, 2007; Larsen and Piche□, 2009; Reeves, 2012; Jarvis and Lister, 2015; Regan et al., 2015; Ritchie, 2015). According to the hallowed phrase, ordinary people as well as financial and corporate sectors have been increasingly invited to become the 'eyes and ears' of national authorities for reporting suspicious behaviours, objects and situations. The multiple and repeat call for the re-distribution of surveillance responsibilities to the 'civil society' has been associated with the advent of a new kind of right, "the right to suspicion" (Bossio, 2005; Chan, 2008). While the pervasiveness of suspicion throughout society has now become a matter of course in the literature, little is known yet about the suspicion-in-the-making in relation to the wide range of potential eyes and ears of the State.

Notwithstanding the illusion of radical novelty, the contemporary "process of blurring boundaries" between state security agencies and the public is marked by a series of continuity and dis-continuity (Lyon et al., 2012: 2). The emphasis on citizen and corporate leads ties in with former programmes of responsibilization designed to enlist non-security professionals in the police and intelligence territory of suspicion, especially in the United States. "Law enforcement has been using some form of SARs [suspicious activity reports] for decades, collected through a variety of mechanisms, including information received from tip hotlines, 911 calls, neighborhood watches, schools and community centers, or police in the field" (Regan et al., 2015: 741). While suspicious activity reporting features prominently in the US repertoire, it has also been subject to a form of universalization in specific areas of policing. In this regard, the fight against money laundering and terrorist financing provides the paradigmatic example of how suspicious activity reporting can become the backbone of policing practices.

First issued in 1990, the Financial Action Task Force (FATF) recommendations are now recognized as the international norms for combating 'dirty money' in over 190 jurisdictions. The reporting of suspicions is the cornerstone of this normative framework transposed into hundreds of national laws. In some countries, everybody is encouraged to become voluntary information providers. In Canada, for example, a federal web form is available to any individual who "would like to provide information on a person or an organisation you suspect is involved in money laundering or of the financing of terrorist activities". Nevertheless, suspicion in the "configuration of financial policing" is less conceived as a right for the public at large than a duty for designated businesses (Amicelle in press). Rather than one tool among many in the anti-money laundering/counterterrorist finance repertoire, suspicious activity reporting has been designed as the Alpha and the Omega for chasing dirty money for over 25 years. Every single national configuration is first and foremost dedicated to the collection and analysis of suspicions submitted by 'reporting entities', from banks to legal professionals (Levi, 1991; Naylor, 1999; Reuter and Truman, 2004; Favarel-Garrigues et al., 2008; Sharman, 2011; Helgesson and Mörth, 2016).

The aim of the working-paper is precisely to shed light on suspicious activity reporting as routine work. The focus on financial policing provides an opportunity to reflect upon the formalization of the 'suspicion-in-the-making' in general, outside police and intelligence organizations in particular. It is worth noting that the configuration of financial policing corresponds to a general trend in surveillance practices driven by suspicion, being "simultaneously more visible and invisible" (Lyon et al. 2012: 3). On the one hand, media coverage of financial scandals and terrorist issues contributes to lend visibility to the follow-the-money methods whereas academic works highlight the rationale of suspicion at the core of financial surveillance. On the other hand, as other monitoring practices, "the actual operation of surveillance, the precise nature and depth of its penetration, along with the protocols for how one is singled out for suspicion or reward are opaque to all but a select few insiders" (Lyon et al., 2012: 3). The working-paper seeks to tackle such an opacity with two questions: Following the premise that suspicion is less an event than a process (Dixon et al. 1989), how do 'reporting entities' produce suspicion for reporting purposes? To what extent the 'quality' of suspicious activity reporting is controlled?

In support of this general proposition, we first provide insights about our fieldwork in Canada's configuration of financial policing and our qualitative research methodology. We then elaborate on the articulation of surveillance, risk and (ab)normality in the production process of suspicion. Next, we highlight two generic situations that ultimately lead to reporting. Finally, we analyse the ways in which quality control of reporting practices takes the form of an argumentative battle between financial policing partners, with an implicit but structural incentive for over-reporting.

Fieldwork and Methodology

In Canada, 31,000 businesses must comply with legal obligations under the Proceeds of Crime (Money Laundering) and Terrorist Financing Act. This includes financial entities (such as banks and credit unions), life insurance companies, securities dealers, money services businesses, accountants, real estate brokers, casinos, dealers in precious metals and stones and British Columbia notaries.1 Legal obligations consist of 'knowing customers', monitoring accounts and transactional activities and eventually reporting transactions to the relevant State authority, i.e. the financial intelligence unit. Canada's configuration goes beyond suspicious activity reporting. Indeed, what must be submitted to the financial intelligence unit includes (a) 'suspicious transaction reports' as well as (b) 'electronic funds transfer reports', (c) 'terrorist property reports', (d) 'large cash transaction reports' and (e) 'casino disbursement reports'. "Unlike all other reporting obligations, there is no monetary threshold associated with the reporting of a suspicious transaction" (Fintrac 2016a). Over 23 million financial transaction reports are submitted annually, with approximately 110,000 suspicious transaction reports, 170,000 casino disbursement reports, 9,000,000 large cash transaction reports and 14,000,000 electronic funds transfer reports (Fintrac 2016b).

On the law-enforcement and intelligence side, 11 federal departments and law enforcement agencies are officially involved, eight of which receive dedicated funding with an overall budget of $70 million per year: (a) the Canada Border Services Agency, (b) the Canada Revenue Agency, (c) the Canadian Security Intelligence Service, (d) the Department of Finance Canada, (e) the Department of Justice Canada, (f) the Financial Transactions and Reports Analysis Centre of Canada (Fintrac), (g) the Public Prosecution Service of Canada and (h) the Royal Canadian Mounted Police (Department of Finance Canada 2015). The critical federal agency is Fintrac as both Canada's financial intelligence unit and regulatory body of reporting entities. Established in 2001, Fintrac has a total of 350 staff for an annual budget of 55 million Canadian dollars. Fintrac's core mandate is to receive and analyse financial transaction reports in order to provide "actionable financial intelligence that assists Canada's police, law enforcement and national security agencies in combatting money laundering, terrorism financing and threats to the security of Canada" (Fintrac, 2016c).

Although suspicious transaction reports account for about 0.5 per cent of the overall reporting, they are presented as the most important reports. "The question is where to look for the needle in a haystack? It is nice to have 20 000 transactions of Mister X in my database but it is the suspicious transaction report that will do 'bang', telling me that 'Mister X is a bad guy'. We will do a disclosure with this because you cannot expect that the analysts will look at more than 22 millions reports that we receive every year. It is the suspicious transactions reports that define the road map for the bad guys" (Interview within Fintrac, 2015). According to Fintrac guidelines, "a suspicious transaction is one for which there are reasonable grounds to suspect that the transaction is related to a money laundering offence or a terrorist activity financing offence. A suspicious transaction can include one that was attempted" (Fintrac, 2017). The banking industry is the major reporter for Fintrac with six "domestic systematically important banks", 22 other domestic banks, 24 foreign bank subsidiaries and 29 foreign bank branches (Department of Finance Canada, 2015: 35).

Our empirical material is precisely related to Canada's domestic banks. The article draws on 30 semi-structured interviews with Fintrac officials as well as chief anti-money laundering officers and related employees in a representative range of Canadian banks. With regards to Fintrac, face-to-face interviews were conducted in the headquarters in Ottawa and in two of the three regional offices (Montreal and Toronto). With regards to banks, face-to-face interviews were conducted in the same cities, either in the headquarters or on the occasion of professional conferences in Toronto, Canada's financial centre; one interview was conducted over the phone. All interviews were recorded with the agreement of the participants and last on average about 90 minutes. They were approached in the light of a quest for the understanding of a social process—the production of suspicion—and its conditions of possibility. In this respect, interviews were directed towards key practices in financial policing and the social representations behind them. Following Howard Becker's (1998) trick, we asked 'how' (and a bit 'what') rather than 'why' to provide a space for expression of interviewees' subjectivity while encouraging them to be as descriptive as possible about their role, relations and practices. As a result, interviews include a series of precisions about critical moments of the studied process depending on the institutional position of each participant.

The selected participants were contacted and interviewed as professionals with unique information. Although they had no reason to lie knowing that we were interviewing people from the same or related institutions, we did not take their words at face value. Different strategies were used to control the reliability of information. As already mentioned, bringing interviewees back to the description of specific events and routine actions constituted a first strategy. Each interview started with the description of participants' role and everyday work. Furthermore, interviews were conducted in two stages. Firstly, ten 'exploratory' interviews were conducted within Fintrac and banks. Their content was helpful as a kind of filter for the following interviews to obtain further details on the same activities while orientating participants towards non-covered issues. The systematic cross-checking of interviews content was critical to deal with potential errors and cover-up attempts while having an overview of practices and related-social representations. From this perspective, the expression of actors' subjectivity was less restrained than 'used' to access to their mode of reasoning in relation to objective and perceived constraints (Pinson and Sala Pala, 2007). In the light of our research questions, the set of interviews contributes to identify and question key moments of the production process of suspicion and report.

1) Financial Surveillance : Risk Management and 'Theory of Normality'

"As a financial institution, we monitor about six million customers, over 150 million financial transactions each month" (Interview within a bank, 2015). To paraphrase Becker about academic research, suspicious activity reporting relies on 'concepts' (risk and (ab)normality) "to know where to look, what to look for, or how to recognize what you were looking for when you find it" (Becker, 1998: 110). Financial policing combines three elements to produce suspicion: (a) a risk-based approach; (b) a theory of (ab)normality; and (c) a surveillance apparatus. This section aims to shed light on the first two elements, in particular (ab)normality, and how they are articulated to surveillance.

Firstly, the risk element is very well known in the literature on money laundering and terrorist financing. Attention has been paid to the risk colonization of the fight against dirty money, from the international adoption to the national implementation and local domestication of the risk-based approach (Amicelle, 2011; Bergstrom̈ et al., 2011). Within this approach, risk-scoring plays a critical role in distributing surveillance resources in accordance with customers' riskiness. A series of criteria is used to calculate every single client's risk-score, including professional occupation, business sector, country of residence, account type, any relation with an entity already defined at risk, any matching with "privately compiled lists of risky banking clients" (De Goede and Sullivan 2016: 67), any previous suspicious transaction report and so on. Each criteria is associated with different possible risk levels and each risk level is allocated to a number of points. Therefore, client's risk-score is calculated based on the total number of points in relation to the criteria and their related-risk levels. The risk-score is interpreted in the light of a risk-ranking system that can include over half-dozen ranks from very low risk to very high risk. The frequency and intensity of surveillance varies from client to client in the light of the risk-ranking. Depending on technological sophistication, 'risk alerts' are automatically produced when client's risk-score is subject to modification. For instance, a client can move from low risk to high risk after being reported to Fintrac once. This example reflects the dynamic and non-linear character of suspicion production. Indeed, one suspicion-based reporting modifies client's risk-score that impacts the specified degree of surveillance to further assemble suspicion for further reporting.

Risk-scoring is a standard practice across the banking industry, but the methodology may vary from bank to bank, starting with the ways of defining the relative riskiness of professions, business sectors, financial products or countries. A chief anti-money laundering officer talked about this at length: "It happens all the time. It is based on the methodology that everyone uses because some people just use it straight. They will get a list from like Transparency International or whoever, and say this is our list of high-risk countries. And they will just be like this is it, we are going with this. Others apply a sort of mathematical formula based on public information that is received. And so you will have differences from bank to bank. Usually they are not that big...but you will have differences based on the methodology that they have in place...and it could be something as little as high-medium or low, and one bank may have medium and the other one may be high. Not to often you will see that one bank has a low and the other has a high" (Interview within a bank, 2015). Given that risk-scoring sets the guidelines for surveillance practices, methodological choices—that overlap with business choices—impact the production of suspicion.

Secondly, while the risk element—through risk-scoring—is crucial to choose where (and who) to look more intensively, surveillance also depends on a theory of (ab)normality to choose what to look for. "The production of suspicion is therefore driven first by a theory of 'normality' : certain objects or people are supposed to be in certain places, doing certain things" (Chan, 2007 : 56). Modes of policing combine risk communication and surveillance to assemble suspicion (Huysmans, 2014), but they also rely on a set of rules to draw "attention to any behavior that disrupt the 'normal'" (Norris ,2003: 265). From this perspective, financial policing agents within banks do not differ from police patrol officers who develop indicators of abnormality in order to take action in the field (Ericson, 1982). Harvey and Lau underline that "the regulatory authorities have elected to use banks to combat money laundering activity on the assumption that laundering activity will be evidenced via some unusual or anomalous account transaction [...]" (2008: 58). The assumption that criminal financial behaviour is distinct and distinguishable from 'normal' financial behaviour is at the heart of financial policing but it is also a matter of debate, especially on terrorist financing (De Goede, 2007; Levi, 2010). In practice, the definition of (ab)normality is pivotal for analysing customers' behaviours and producing internal alerts that may lead to suspicion-based reports. As we will describe in great detail, Canadian banking actors rely on various strategies, modes of reasoning and sources of information to define and differentiate 'normal' financial behaviours from the 'abnormal'.

Indeed, Financial institutions have to "capture activity conducted by customers that is outside the normal or expected activity" (Protiviti, 2013 : 1). But activity expected by whom and normal where, when, for what and for whom ? "Identifying the normal activity is a challenge many institutions face […]" (ibid.). Such a challenge is increased by the fundamental premise that criminals and terrorists want to present a semblance of 'normal' daily routine in order to mask their intentions and become indistinguishable from any other banking customer. Responding to such dissimulation strategies requires banks to observe clients and their behaviors below what they show. How do financial institutions try to set an operational representation of (ab)normality in the context of a reinforced risk-based monitoring system ? Although "'abnormality' has entered our everyday discourse with a conceptual force that seems both natural and inevitable" (Foucault, 2003 : xxv), its definition and delimitation is far from straightforward in practice.

According to official guidelines for financial policing, the abnormality lying at the basis of suspicion is not an abnormality of nature but an abnormality of behaviour. Fintrac officials remind reporting entities "that behaviour is suspicious, not people" (Fintrac, 2017 : 15). It is critical to understand how the idea of (ab)normality is approached within banks, and how it is operationalized as the filter for analysing customers' behaviours. Two modes of inferential reasoning (deduction and induction) and three scales of observation (the bank population ; the peer-group ; the individual client) are privileged for distinguishing 'normal' and 'abnormal' behavioral patterns in a given time and space.

1.1) When the Abnormal Comes First

Under the framework of the traditional and still dominant approach in the field of financial policing, the abnormal comes first to stimulate deductive reasoning and the scale of observation varies from the general banking population to any particular client. In concrete terms, generic indicators of abnormality are provided to financial institutions in order to draw inferences believed to identify those who may be suspected of money laundering or terrorist financing. Indicators are selected as distinctive features to support monitoring practices. This approach is not a Canadian specificity, and certainly not a specificity of financial policing. The FBI advisory on suspicious letters or packages is but one example of official state publications with indicators of abnormality (https://prochoice.org/wp-content/uploads/fbi_mail_advisory.pdf ; Chan, 2007).

In Canada, Fintrac is the national provider of indicators "to help assess whether or not transactions might give rise to reasonable grounds for suspicion. They are examples of common and industry-specific indicators that may be helpful when evaluating transactions, whether completed or attempted. They include indicators based on certain characteristics that have been linked to money laundering or terrorist activities in the past. These indicators were compiled in consultation with reporting entities, law enforcement agencies and international financial intelligence organizations" (Fintrac, 2017 : 17). The set of generic indicators of abnormality thus derives from the aggregate experiences of state agencies and the vast array of reporting actors who have been involved in financial policing over the years in Canada and abroad. This shared-recipe knowledge about what to detect is communicated to help establish suspicion for both money laundering and terrorist financing even if "there are some small differences between money laundering and terrorist financing indicators. For example, amounts relating to terrorist financing generally may be smaller. However, there is no distinction made in the indicators" (ibid. : 16).

The provision of official indicators of abnormality

What are these indicators ? On the one hand, "common indicators" are intended for all reporting entities from banks to dealers in precious metals and stones. The eight categories of 118 common indicators are as follows :

1) The category **General** comprises 32 indicators such as "Client insists that a transaction be done quickly".

2) The category **Knowledge of reporting or record keeping requirements** comprises 8 indicators such as "Client has unusual knowledge of the law in relation to suspicious transaction reporting".
3) The category **Identity documents** comprises 12 indicators such as "All identification documents presented appear new or have recent issue dates".
4) The category **Cash transactions** comprises 16 indicators such as "Client conducts a transaction for an amount that is unusual compared to amounts of past transactions".
5) The category **Economic purpose** comprises 8 indicators such as "Transaction seems to be inconsistent with the client's apparent financial standing or usual pattern of activities".
6) The category **Transactions involving accounts** comprises 21 indicators such as "Account that was reactivated from inactive or dormant status suddenly sees significant activity".
7) The category **Transactions involving areas outside Canada** comprises 12 indicators such as "Use of a credit card issued by a foreign bank that does not operate in Canada by a client that does not live and work in the country of issue".
8) The category **Transactions related to offshore business activity** comprises 9 indicators such as "Accumulation of large balances inconsistent with the known turnover of the client's business, and subsequent transfers to overseas account(s)".

On the other hand, "industry-specific indicators" are dedicated to each kind of reporting sector. Most of the banks can be connected with five of them, for a total of 160 possible indicators.

First of all, as **financial entities**, banks rely on three categories of 65 specific indicators which are differentiated as follows :

1) The category **Personal transactions** comprises 27 indicators such as "Client requests movement of funds that are uneconomical".
2) The category **Corporate and business transactions** comprises 29 indicators such as "There is a sudden change in cash transactions or patterns".
3) The category **Transactions for non-profit organizations (including registered charities)** comprises 9 indicators such as "The non-profit organization has operations in, or transactions to or from, high-risk jurisdictions".

Second, as **businesses who send or receive electronic funds transfers, or remit or transmit funds**, banks rely on another category of 33 specific indicators such as

"Country of destination for a wire transfer is not consistent with the nationality of the individual client".

Third, as **businesses who provide loans**, banks also rely on a category of 15 specific indicators such as "Client repays a long term loan, such as a mortgage", within a relatively short time period'.

Fourth, as **life insurance companies, brokers and agents**, banks rely on another category of 22 specific indicators such as "Client shows more interest in the cancellation or surrender of an insurance contract than in the long-term results of investments or the costs associated with termination of the contract".

Finally, as **securities dealers**, banks rely on 25 other indicators such as "Transaction of very large dollar size".

As a result, any bank falling in all of these categories has 278 different official indicators of abnormality available to them (118 common indicators + 160 industry-specific indicators). Approximately eighty-five percent of them define the abnormality in one way or another (for instance, "Client is accompanied and watched"). They are designed in very general terms to be tested against the behaviour of any member of the bank population in the first instance, regardless particular knowledge in relation to individual customers. As noted by Jef Huysmans in other policing contexts, motivational indications of committing a crime are not what immediately matters (2014 : 105-106). Client knowledge should be considered subsequently in the evaluation process, to the extent that "the presence of one or more indicators as well as [the] knowledge of [the] client's business or financial affairs may help [banking actors] identify suspicious transactions" (Fintrac, 2017 : 18). By contrast with the vast majority of indicators, about fifteen percent of them are tautological, since they do not define the abnormality as such (for instance, "Transaction appears to be out of the normal course for industry practice […]"). In other words, transaction appears to be abnormal because it is out of the normal. Those tautologies require more extensive analysis by banking actors who must clarify for themselves what is 'the normal course for industry practice'. The tautological indicators can easily be recognised to the extent that they interchangeably include terms such as not normal, atypical and unusual. Furthermore, they mainly refer to a temporal meaning of abnormality that depends on client knowledge. For instance, the "[c]lient starts conducting frequent cash transactions in large amounts when this has not been a normal activity for the client in the past".

In addition, in Canada, as in other countries (on Switzerland, see Palmieri & Rigotti, 2014), Fintrac guidelines caution that "a suspicious transaction may involve several factors [indicators] that may on their own seem insignificant, but together may raise suspicion that the transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both" (Fintrac, 2017 : 15). In other words, there is an official incentive to combine together several indicators of abnormality to perform financial policing. This remark leaves important discretion to banking actors, especially with respect to the creation of pre-defined alert scenarios based on their own combination of indicators. In the case of scenarios with only two indicators, the total set of 278 indicators might already give rise to 77,284 possible combinations. It reaches 21,484,952 possibilities with the association of three indicators and the differential weighting of each criteria can increase considerably those possibilities, even before another indicator is added. More generally, the Canadian regulator promotes the articulation of linages between indicator(s), client knowledge, and context (Fintrac, 2017 : 18).

Indicators of abnormality, client knowledge and context : A critical assemblage

With regards to client knowledge, the very form and content of knowledge may vary from one bank to another and from one type of clientele or business relationship to another. According to Lyn Loftland (1973) and John Dewey (1938), human beings can develop a knowledge of people (acquaintance-knowledge) or a knowledge about people (knowledge-about). In connection with surveillance and control, Clive Norris sums up this distinction by reminding that the "basis of knowing of, rather than about people, is face-to-face interaction". When we only know about people our knowledge is secondhand' (2003 : 251). With reference to banking relationships, the frequency of face-to-face interaction and the predominant form of client knowledge may depend on the ways of doing business and clients' habits (from client's frequent visits to a bank branch to exclusively online banking), the size of bank branch, its location (from small rural areas to densely populated urban areas) and the type of financial services (from basic chequing account to wealth management products). In Canada, the banking industry at large and even within the same financial institution, there is a wide gradation from extensive acquaintance-knowledge of people to documents-based knowledge about people. It also means that there is an infinite variety of financial policing in the field with different abilities to make sense of behaviours in the face of indicator(s), knowledge and context.

Then, with regard to 'context', "the context in which the transaction occurs or is attempted is a significant factor in assessing suspicion. This will vary from business to business, and from one client to another. You should evaluate transactions in terms of what seems appropriate and is within normal practices in your particular line of business, and based on your knowledge of your client" (Fintrac, 2017 : 15). Thus, according to the regulator, the qualification process of suspicion should not be limited to a set of behavioral indicia of abnormality viewed in isolation and in an abstract manner. It should also depend on each concrete situation, in relation to each bank's activity portfolio, as well as each client's banking history and possibly known attitude at the counter. The process should be based on prior knowledge, careful ongoing monitoring and the time and place of the observed behaviour (on comparable issues regarding street stops of citizens by the police, see Alpert, 2005 ; Fagan and Geller, 2014). At the end of the day, the production process of suspicion becomes a much more complex exercise of interpretation than checking boxes on an official list of X behavioral indicators of abnormality with X potential combinations.

Finally, it has to be mentioned that reporting entity maintains a margin of manoeuvre in selecting all or part of official indicators and adding others, with variations from bank to bank depending on their activities, needs, resources and contacts. Indeed, each financial institution is involved in a DIY work to compile their own set of indicia, in order to reflect their type of customer, their business situation and their position in the industry. Consequently, the range of selected abnormalities slightly differs from one bank to another. Nevertheless, once selected and written into internal policies, the indicators render banking actors accountable in the case of an examination conducted by the regulator. As a Fintrac official said : "We challenge them and we say, your indicators say that if a person comes in and refuses to provide identification, and don't conduct the transaction, that's suspicious enough that you report it. It is part of what you have documented. And here is a situation that has happened, and you did not report it. Why didn't you report it ? Usually, it's silence" (interview within Fintrac, 2015).

The largest banks receive further indicators directly from law enforcement agencies that share their confidential typologies, especially on terrorist financing, that can be related to very small amounts of money from a legal origin. Additional information on terrorist activity financing has been increasingly exchanged as strategic priorities have evolved over time. "We have done two, three 'workshops' since last year with the biggest banks to deepen the notion of suspicion in the antiterrorist domain. It is easier for them to understand with real examples ; the events of Ottawa, Saint-Jean and Charlie Hebdo in Paris, here are the loopholes, here is your possible contribution and here are the indicators of terrorist of interest for us in this particular case. It is a question of deepening the existing indicators. It is essentially a zoo of indicators if I may say so. There are the general indicators, same thing for a police officer about dubious behaviours on the street. The police officer has learned them at the Police academy and then he joins a specific, specialised team and he will have other more specific indicators. We are doing the same for anti-money laundering professionals" (Interview with Fintrac, 2015). Regarding terrorist financing, the traditional focus on financial support to foreign terrorist entities still persists but it is supplemented by the desire to keep watch over the money potentially used in Canada for planning an attack on the national territory or for travelling abroad to join ISIS foreign fighters.

"Like a typology could be institutions or sort of looking at an individual who buys a credit card, buys a fare to Turkey or somewhere else like that. Basically travels over there and then you see that they are making purchases, and then they disappear, from that perspective. So, you have a typology, you sort of search everybody who bought a plane ticket to that area and what they did since that point and time" (Interview within a bank, 2015). In this context, Fintrac officials have also insisted on additional indicators to target both 'high-risk travellers' and 'radicals'. Some of those indicators were reported in the press last year (La Presse, 2015), including : **1) for potential canadian 'foreign fighters'** : travel-related expenses (flight ticket, entry visa, passport) ; bank account that has been emptied ; the sale of personal possessions ; access to a Canadian bank account from a high-risk area ; a client publicly identified as a high-risk traveller ; and **2) for potential 'radicals'** : donations to a cause publicly considered as problematic ; unusual purchases (weapons, ammunition, ammonium nitrate products, propane, acetone) ; rapid repayment of debts ; public online activities supporting acts of violent extremism ; a customer who announces a date for closing bank account.

Everything is slightly different from one bank to another, regarding the production and access to internal and external indicators. But the rationale remains the same. It involves a deductive reasoning which firstly consists in stating what is the abnormal in general and then starting from there to draw inferences about actual transactions. Although this remains the dominant approach in the field of financial policing, banking actors also have developed a second framework of analysis, in which the normal comes first via the use of a inductive mode of reasoning.

1.2) When the Normal Comes First

“They [Fintrac indicators] are not intended to cover every possible situation […]” (Fintrac, 2017 : 17). The translation of such an official statement into practice leads to two ad hoc orientations in the ways banks currently draw the contours of the (ab)normal. On the one hand, this statement is interpreted as an incitement to look for additional indicators. As already mentioned, numerous banking actors follow this path with their own compilation of extra indicators coming from external sources and internal experience. On the other hand, it is interpreted as the confirmation that the quest for indicators of abnormality is both endless and insufficient. “Increasingly, regulators recognize that rules [scenarios based on indicators] alone are not an effective manner of detection and are pressuring banks to include more sophisticated analytic routines” (Conroy, 2015 : 51).

From this perspective, another analytical trend is developing in the reverse direction of the traditional approach in which the abnormal comes first to stimulate proto-deductive reasoning. Under the framework of the second approach, it is the normal that comes first to stimulate inductive reasoning, and the scale of observation is mainly the ‘peer-group’. In concrete terms, the aim is to determine first what is the ‘normal state’, to be able to detect subsequently any behaviour that deviates from it and draw inductive inferences believed to identify those who may be suspected of money laundering or terrorist financing.

To some extent, this second approach recalls the analytical demarche carried out by Émile Durkheim, one of the founders of sociology. According to Durkheim, the sociological meaning of normality depends on the generality of social phenomena (1895). A fact is deemed sociologically normal if it reaches a certain degree of generality in terms of frequency and regularity. He specifies that the normal state of things cannot be defined in the abstract and in absolute terms. The normal state can be only determined in relation to a specific social species in a given time. This entails constituting and classifying social species first. To apply the sociological analogy to this kind of financial policing, the second approach consists in grouping together clients into different species on the basis of one or more common attributes. This is done in three ways, depending on the banks, that are not mutually exclusive.

The constitution and classification of client “species“

A-The constitution of a global species.

First, banking actors, often with limited analytics, can consider their entire client population as one species (i.e., one peer-group), all things being equal, or more generally two species with the simple separation between physical and legal persons. In this context, they calculate ‘global behaviours’ and then aim to flag what related to whom is situated at the margins of the clientele majority in the statistical unit. “One of the ways we do a global behaviour is we say what’s the amount of cash deposited in the entire system over the course of twelve months. January 1st, to December 31st… How much cash? We take that. We identify and we break down the 90th percentile, to the 99th percentile value. We basically say the 90th percentile of a single deposit, that is $5,000, then that’s my threshold. I’m setting the threshold at the 90th percentile, which means anybody who’s below 90%, if you’ve deposited up to $4,999, it’s not going to trigger, because 90% of the people who do a deposit, personal versus non-personal, you’ve identified the 90th. And anything between 90 and 99, it starts being closer to be a bigger issue” (Interview within a bank, 2015). This ‘one-size-fits-all methodology’ faces criticism from many banking actors, and vendors of transaction monitoring technologies, for not paying attention to the heterogeneity in banking population. According to the critics, the various forms of global determination of the normal leads to poor alert coverage within the bank population, as well as an escalation of alerts and hence too many false positives. Here, the issue at stake is less the statistical methods used, than the way of constituting a range of peer-groups.

B-The constitution of cultural species.

Second, a form of culturalism exists to assist the business lines in determining what could be interpreted as normal for specific cultural peer-groups. “The other fun part was bridging the culture element and understanding how certain cultures just actually deal with money. The Asian culture, for example, and even the Indian culture, specifically if you’re talking about certain events in life… The Chinese culture, in and around Christmas, and anytime they get married, it’s an envelope full with money. It’s never a gift, it’s never a blender, it’s cash. So if some young couple walks in and says, I just got married, here are $30,000… that’s a legitimate answer” (Interview within a bank, 2015).

Similar comments were made by other chief compliance officers during interviews on the 'Italian culture', the 'Haitian culture' and so on, to capture and classify clients in relation to diverse community identities. With reference to the 'culture element', they want their font-line staff members to put themselves in the shoes of clients belonging to 'different cultures' in order to differentiate and adjust the definition of normal behavioural pattern. "You have to explain there is actually different cultures and different cultural things. Yes, that kind of training, when you are trying to say to them, I need you to look for money laundering but understand that there are certain things that look like money laundering but it's not" (Interview within a bank, 2015).

However, this informal effort to create cultural groupings is based on common sense observation at best and on stereotypes at worst. Furthermore, it may lead bankers to a paranoid mindset, to the extent that compliance officers also insist that criminals will use the same so-called cultural characteristics to avoid suspicion. For instance, one interviewee was very wary about determining whether a woman from the 'Italian-canadian community' was really making a large cash deposit because of her wedding or in relation to a criminal-related activity under the official excuse of an Italian-style wedding. In a similar vein one interviewee said: "You always say watch out for large transactions but take this example. A grandmother died. So the family goes in, they might go back to the house and start cleaning up. And there are multiple instances when they come back and they have $98,000 in cash, just plucking under the counter. So, here you go, this was in her house because she stashed it everywhere. Because they [abstract reference to the elderly persons of a specific cultural community] don't trust banks. So, normal… Those are extreme examples, but the problem is people also know that those exist, so they will come in and say those are funds from my grand-mother's house. She died last week. Here's $50,000. And then the question is, we always look at what happens after that" (Interview within a bank, 2015). Here, the integration of the 'culture element' is, to a certain extent, 'cancelled' by the concern that it can be abused by criminals. However, this does not mean that the culturalist analysis disappears. It is only displaced from the cash deposit to the monitoring of the expected cultural way of using the so-called grandmother's inheritance.

C-Towards the algorithmic constitution of transactional species.

Third, the (largest) banking actors increasingly rely on analytics to develop 'dynamic segmentation strategies' promoted by vendors of monitoring technologies in the name of "more analytically rigorous peer-groups" (Conroy, 2015: 16). "Segmentation is the process of grouping together customers and accounts that have similar characteristics and transactional behaviors […]. Segments of customers and/or accounts may be grouped together based on one or more of their inherent characteristics, such as average transactional amount, average transactional volume, net worth, product usage, region, customer/account type, etc." (SAS, 2015: 1). Besides the issue of (ab)normality, it has to be noted that such a segmentation model feeds into the process of risk-scoring that modulates the frequency and intensity of financial surveillance. "It is important to keep in mind the bank's ultimate goal in building the segmentation model(s) – to allow for effective risk-based transaction monitoring by applying different threshold values to different groups of customers" (ibid.; on risk and transactions, see Amoore & De Goede, 2008). Performing such a peer-group segmentation depends on three main tasks.

First of all, banking actors must select a set of data points (i.e. the 'inherent characteristics') to develop their own segmentation model. This selection is critical before conducting "data discovery" (SAS, 2015), because data will only speak in accordance with the formulated questions and expressed interests of each financial institution. The first step thus consists in designing the suitable clustering algorithm, i.e. the series of instructions that would allow a result to be obtained (for a sociological account of algorithms, see Cardon, 2015). To do so, two types of attributes are used separately or together for the purpose of constituting homogeneous species.

On the one hand, traditional characteristics of sociological, marketing and social policy interests - such as 'income' and 'geography/location' - are still mobilised for classifying people and segmenting the population. Besides algorithmic calculation, socio-demographic attributes are also used to assist the business lines in another non-culturalist form of common sense observation. "It is one of the things we would always talk about. Look at the profile of the customer when you pull out a transaction. Look at the profile. Look at how old they are. What do they do for a living? Where is their address? If you are in one side of the city and they live at the complete opposite side of the city, why are they banking with you? And generally my question would be, do they work down the street? Oh yeah, they work down the street at the flower shop or something. Then that's the reason why they're banking with you. But other than that it's abnormal" (Interview within a bank, 2015).

On the other hand, transactional characteristics are adopted to segment the bank population on the basis of financial conduct. The attribute 'transaction types' is one of the most common data points, “generally used in combination with either transaction amount or count” (SAS, 2015: 5.). The ‘transaction type’ can be credits and/or debits and they are analysed in association with variations in volumes (amount and/or frequency) of funds. Thus, the bank population is both represented and disaggregated into a cloud of selected data points. The aim is to form relative homogeneous segments (peer-groups) on the basis of minimum distance between selected data points for each segment.

While eminent scholars have stressed the key difference between two forms of knowledge regarding people (of / about) (cf. subsection 1.1), another distinction emerges between two forms of knowledge about people. The use of socio-demographic criteria refers to a conception of knowledge about people in terms of pre-defined social identities. ‘You know’ about people because you ‘know’ who they are socially. Here, social classes are mainly inferred from economic attributes while national, cultural or ethnic affiliation are mainly inferred from geographic attributes. By contrast, the use of transactional metrics refers to a conception of knowledge about people in terms of their daily conduct. ‘You know’ about people because you ‘know’ what they do. Here, their behavioural pattern is inferred from their past transactions, regardless any socio-demographic knowledge about them. As argued by Cardon (2015: 37), “persons tend to disappear behind their traces” of transactional conduct since classic elements of their identity (name, biographical data, profession, administrative, civil and social status) are of no interest to know about them. Ultimately, different kinds of peer-groups will emerge depending on the choice of characteristics, from the constitution of socio-economic classes to transactional species. Although these two types of knowledge are often opposed in the academic literature, it is not necessarily a zero-sum game in practice. It would be premature at this stage to outline the predominance of one type of ‘data points’ over the other in the field of financial policing.

Second, once selected, the data points are used to explore the customer database (i.e. data discovery) with statistical/analytical methods in order to segment the entire bank population into smaller and more homogeneous groups. Analytic devices are utilised to create peer-groups from as low as hundred customers, based on patterns in their transactions and/or socio-demographic similarities.

Third, results of the data-driven, knowledge discovery phase are subject to refinement and validation procedures concerning the expected homogeneity (i.e. internal similarity) of segments in relation to the bank's objectives. Ultimately, 'normal' behaviours are induced depending on their degree of generality for each constituted peer-group on the basis of the recorded transactions. This method requires constant re-evaluation for necessary updates of the 'normality', in light of the evolving transaction dynamics, but it is certainly not always the case in the field. In other words, the normality established per constituted species is often outdated.

"The primary reason to develop a peer group model is to allow for anomaly detection at the peer group level. […] The ultimate goal of monitoring activity at the peer group level is to identify customers who are expected to behave in a similar fashion as other customers (i.e., the peers) – but don't" (SAS, 2015: 4). As noted by Dominique Cardon about internet users, the expected activity of the banking customer is predicted by the past activities of those who look like him or her in terms of transactional conduct. The normal is relational, not in terms of 'real' transactional contacts between people, but in terms of behavioural affiliation to the other. Then, information on past behaviour of same segment of customers – historical data is critical here – is used to define as abnormal any transactional pattern that is deviating from the learned behaviour as abnormal. In the case of transactional species with a cloud-based representation of data points, such as transaction type and volume, it means that any particular transaction-related data that 'significantly' moves away from the center of the cluster would be considered an outlier, as abnormal behaviour within the peer-group. At the same time, the focus on peer-group does not necessarily mean that the 'fine grain of individuality' is being abandoned.

Towards particular understandings of the normal and the abnormal

As promoted by vendors of transaction monitoring systems, "analytical models include historical behaviour profiling and peer group segmentation, to detect unusual activities by comparing customers to their individual historical activity and peer group" (Nice Actimize, 2015: 2). Although "the dynamic measurement of what people 'actually' do" (Ruppert, 2012: 122) is associated with the constitution of transactional species and calculation of their normality, it is also used to define individualized forms of normality on the basis of transactional regularities. As scales of observation, the peer-group and the individual are closely intertwined, as complement and counterpoint. Besides peer-group dynamics, the expected activity of the individual customer is simultaneously thought to be and anticipated as the reproduction of his/her past conduct (Cardon, 2015). “So part of the job of the financial intelligence unit of the bank is that you are monitoring transactions. So you would know, at the end of every month the client gets a paycheck on this date and this date. He pays his rent. He pays his mortgage. He buys gas. The system is monitoring the transactions. Everything is moving along fine. All of a sudden, he receives a $10,000 deposited in his account. Unusual. So, it flags your account but it does not create a notice. It just flags it to watch for it again. So in one week he receives $10,000 and he receives another $10,000 again the following week. So what happens is the system says ‘okay, well this is really weird. Let’s just kick it out for someone to have a look at it’. It is just a flag of unusual transaction. It is within the team,it is just flagging transactions to say watch this. This is kind of unusual because we watch the patterns of the last twelve months and we’ve not had a transaction like this before. So now, have a look at it. Could it be he got married and he received… whatever the case may be. Or someone died and he has inherited. So, it is not saying that it is unusual. It is just saying that it is unusual for the account” (Interview within a bank, 2015).

Overall, the inductive reasoning of the ‘second approach’ – when the normal comes first – leads to a preference for a particular understanding of the normality and, by extension, abnormality. Here the normal behaviour is nothing else than the usual, the regular and the frequent, while the abnormal behaviour is relegated to the unique, the unaccustomed, the outlier. In this respect, it is interesting to note that internal bank reports for investigation that may ultimately lead to suspicious transaction reports to Fintrac are termed ‘unusual transaction reports’. However, this is not as simple as it may first look, and the idea of a systematic overlap of meaning between (ab)normal and (un)usual is being debated in the field of financial policing. As recalled by Fintrac officials as well as in other national and international guidelines (FATF, 2004; JMLSG, 2017), a transaction which appears abnormal or unusual is not necessarily suspicious. “Well, we often say that just because a person has always done a transaction that way doesn’t mean that it’s not unusual. So, you’ll see that option in the credit union sector for instance. The amount of money that goes through that sector is phenomenal. But they have, they call them members, because they own a piece of the union, so it’s a member, and they’re very adamant that it’s a member. It’s not a client or a customer. And they’ll say: but they’ve been doing those types of transactions for years. So, it’s trying to get them to understand that just because they have a relationship with the person doesn’t mean that they can’t be doing something unusual. But going back to what your question was, often they’ll say I’ve never seen them before, so for me that’s suspicious. But it's not because you have not seen them before that it is unusual" (Interview within Fintrac, 2015). "This is normal because it is as usual. No, not always" (Interview within Fintrac, 2015). This concluding quote highlights the complexity, tensions and contradictions of ongoing attempts at determining and weighting simultaneously not one form of (ab)normality but a set of generic, global, categorical, relational and individual (ab)normalities.

Once defined, each bank's theory of normality contributes to detecting practices. Indeed, efforts to distribute 'normal' and 'abnormal' behavioural financial patterns for risk-based surveillance purposes generate alerts. According to their nature and content, indicators are primarily destined for banks branches employees or compliance units and high-tech devices of surveillance located in headquarters.[1] As enigmas, alerts attract attention for further investigation to the extent that they contrast with the way things should be in the 'normal' course of events (Boltanski, 2011). They must be investigated and resolved—to a certain extent at least—in order to better 'qualify' the detected abnormalities for acting accordingly. Every single alert does not automatically lead to a suspicion-based report. The resolution of enigmas represents another pivotal moment in the development of the suspicion process. It results in two opposite outcomes with the translation of the detected abnormality into a false-alert or a suspicious behaviour that must be reported.

2) From Internal Alerts to Official Reporting of Suspicious Transactions

2.1) The Resolution of Enigmas

"The operational units are making sure that we are following the procedures in place, that we are doing everything in a regulatory perspective, such as filing our suspicious transaction reports, filing the large cash currency transaction reports in Canada. So, the majority of our people on anti-money laundering and terrorist financing are in those operational units. And within those operational units, the majority is in our financial transaction units, which are responsible for the STRs reporting" (Interview within a bank, 2015). The resolution of enigmas is assigned to analysts who have to consider all internal alerts, from the 'unusual transaction reports' from branch employees to the

[1] In this regard, staff training, the domestication of indicators in bank branches and the appropriation of high-tech devices are also critical elements in the production of suspicion that are beyond the scope of this article.

'automated alerts' from transaction monitoring devices. Analysts are fully involved in the decision-making process that may ultimately lead to the reporting of the flagged customer's behaviour.

"We have 30 000 to 35 000 alerts a month globally [not restricted to Canada]. Out of those, I would say 2000 to 2500 might result in STR filings" (Interview within a bank, 2015). According to our fieldwork, banks in Canada claim to report from 1 to 25 per cent of alerts for a total number of suspicious transactions reports from few hundreds to several thousands annually. In other words, 75–99 per cent of detected abnormalities are either re-normalized because of manifest human or technical errors of assessment or considered as non-problematic or inconclusive. Bigger the bank is and bigger seems to be the rate of non-reported alerts: "Between transactions alerts, names hits and economic sanctions hits, there's about 3.2 millions alerts last year that we have processed that translated to approximately 55 000 cases for investigation" (Interview within a bank, 2015). A case for investigation does not necessarily lead to a suspicious transaction report, but it means that the alert is considered as serious enough for in-depth investigation rather than being dismissed almost immediately.

The investigation can take various paths and may vary in magnitude. First of all, dedicated analysts go through the client's account to see what happened and set the context for the alert, especially for automated alerts from transaction monitoring devices. As mentioned by a chief anti-money laundering officer, "they take a more holistic view of the account to see if this transaction makes sense, given everything that this client has done. So they do go back and look at what the client has been doing from that perspective. They will do that aspect and then, from there, they will basically determine whether or not it was suspicious" (Interview within a bank, 2015). They can also contact the bank branch where the flagged client is to get details. They investigate and if they still cannot corroborate or figure out why that transaction happened, they go further or send the case to another line of investigators who will go further with the extensive use of open-source information. This includes news articles and social media platforms—starting with Facebook—as well as public registers and online access to civil, criminal and penal judicial records. In some cases, banks send letters to the flagged client to get clarification as to what was the purpose of the transaction before determining that it was suspicious.

The degree of subjectivity associated with suspicion-based models of intervention is not denied within reporting entities. On the contrary, interviewees from banks all emphasize this aspect they present as the prime example of the difficulty of their task. As mentioned by one of them, "there is always going to be issues around how much data you have and how much data you need in order to make something appear suspicious" (Interview within a bank, 2015). The lack of certainty and consensus as to how much data and, by extension, "how much suspicion" is needed to act accordingly is a shared-concern in the broader field of policing, from street stops to counterterrorism practices (Alpert et al., 2005; Fagan and Geller, 2015; Stalcup, 2015). Interpretive variations between and within banks are made explicit: "We hit a core issue that is facing the financial sector. Somebody look at the transactions and he may say, Okay, they bought a ticket to Turkey. That's suspicious enough for me. But you look at another institution and they will say no, that's not suspicious. They bought a ticket and so what…I need more information to say that this is indicative of a terrorist finance activity or something that's going to happen. And you can have that taking place within your bank. You can have two investigators sitting next to each other and one will say, you know what, that's suspicious and the other one could say I need more information…or your could have more investigators saying, Okay, let's look at the customer and they may do a deeper dive and say, no, I don't think this one is suspicious. I'm not going to file an STR. And that's what the problem is because… it is an issue when you start to look at terrorist financing or you start looking at suspicious transaction reporting because, suspicious you know that could be normal for me and you could look at it and say, no, no, no, I don't like this activity. It's suspicious to me. It is very subjective" (Interview within a bank, 2015). Along these lines, financial policing agents within banks are keen to insist on the degree of uncertainty that would characterize the ultimate outcome of the suspicion process. However, the transformation of an investigated case of abnormality into a suspicious transaction report is much more ordered across the banking industry than appears at first sight.

Paths of suspicion: towards a hunch-based model?

Regardless of existing and perceived differences and divergences across the banking industry, only two generic—and opposite—alert situations lead to suspicious transaction reports.

Firstly, a transaction is reported as suspicious when the internal investigation is considered as closed, often quickly, with one 'obvious proposition' to resolve the enigma. This was perfectly summed up by a compliance officer: "When there's a structuring type of activity that takes place, that's a definite. You know what, you try to evade the required requirements. We see it, we will file it. When you see something that obviously somebody is trying to violate or try to avoid a required reporting requirement, that will automatically lead to a STR file [...] When you see something in the news, a narcotic rings or arms smuggling rings gets taking down and you see it, and the next day you have that individual or that company as a customer and their activity sort of, and what they say in the law enforcement sort of match it up. Automatically you are going to file a STR and probably reach out to law enforcement. So those types of things will trigger automatic filings" (Interview within a bank, 2015). Here, reporting is motivated by reporting entity's high degree of certainty about the criminal nature of client's activities. More than a reasonable ground to suspect, chief anti-money laundering officers and related employees believe to have proof based on concrete evidence to support their interpretation. They act as if they do report crime rather than suspicion of crime. The alert is deemed to be an obvious case for reporting when it is triggered by what Gold and Levi coined "the visibly suspicious" and "transferred suspicion" (1994). "The visibly suspicious" refers to unsophisticated transactions involving known individuals, i.e. petty crooks barely competent in money-laundering schemes. "Transferred suspicion" is based on external information about the flagged client or affiliates, including negative news in the media, law enforcement requests as well as judicial orders and judicial records. This type of information is used on a daily basis to initiate, support or finalize suspicion of money laundering or terrorist financing. This routine use, however, raises critical questions. For instance, should suspicious transaction reports be by-products derived from criminal charges, even when charges go back many years or were dropped?

Secondly, a suspicious transaction report is also sent in the exact opposite situation, when it seems to be impossible to close the investigation and get any 'obvious proposition' to resolve the enigma. One common narrative emerged from all interviews to characterize this kind of situation, i.e. 'it does not make sense'. This is reflected in similar quotes across interviews: "We do not have any idea what the predicate offense is. This just does not make any sense" (Interview within a bank 2015). "It does not make sense from our perspective" (Interview within a bank, 2015). "There's no logic. There is no banking logic to that" (Interview within a bank, 2015). "The question you are going to ultimately ask yourself is, does this transaction make sense for this customer" (Interview within a bank, 2015). "Why would that make a good business sense?" (Interview within a bank, 2015). "They believe that something is going on. They don't know what. But they just want to tell us about it" (Interview within Fintrac, 2015). The 'does not make sense' narrative is omnipresent in the field of financial policing as a trigger for reporting practices. Here, report is motivated by reporting entity's incapacity to understand client's behaviour. Contrary to the first situation, analysts from operational units and their chief anti-money laundering officer do not have any sense of certainty. Despite in-depth investigation, the enigma is not resolved but it is precisely this non-resolution that leads to a report.

From the obviousness of an alert situation to the senselessness of another, what do the two opposite 'trigger points' of reporting tell us about the contours of suspicion in practice? Following Levi's recommendation to take the distinction favoured by Interpol seriously, a suspicious transaction is conduct which, "because of the circumstances, have reached a level of suspicion sufficient to identify a criminal offence (e.g. subject is suspected of money-laundering and drug trafficking or other stated offence)" (quoted in Levi, 2005: 266). An abnormal or unusual transaction on the other hand "is one or several transactions of an unusual nature but where a criminal offence has yet to be determined" (ibid.). In Canada, part of the so-called suspicious transactions reports rather correspond to the Interpol definition of unusual transaction. Any conduct lying outside determined normalities or matching with pre-defined abnormalities tends to be reported when financial policing agents do not understand and cannot explain why this is so. Paradoxically, this lack of explanation—or the lack of credibility associated with client's explanation if questioned during the investigation—explains the reporting. In this case, suspicious activity reporting relates to a specific inferential mode of reasoning: abduction.

Unlike deduction and induction, abduction is described as the inference to the best explanation. Take one example of abductive reasoning from a different context: "You happen to know that Tim and Harry have recently had a terrible row that ended their friendship. Now someone tells you that she just saw Tim and Harry jogging together. The best explanation for this that you can think of is that they made up. You conclude that they are friends again. [...] the conclusions do not follow logically from the premises. For instance, it does not follow logically that Tim and Harry are friends again from the premises that they had a terrible row which ended their friendship and that they have just been seen jogging together; it does not even follow, we may suppose, from all the information you have about Tim and Harry. Nor do you have any useful statistical data about friendships, terrible rows, and joggers that might warrant an inference from the information that you have about Tim and Harry to the conclusion that they are friends again, or even to the conclusion that, probably (or with a certain probability), they are friends again. What leads you to the conclusion, and what according to a considerable number of philosophers may also warrant this conclusion, is precisely the fact that Tim and Harry’s being friends again would, if true, best explain the fact that they have just been seen jogging together” (Douven, 2016). In the context of financial policing, bank investigators look at a behavioural abnormality and, in the absence of obvious explanations and logical articulation with premises, the much simpler, ‘natural’ and therefore (they conclude) much better, explanation of that abnormality is a link whatsoever with suspicion of illegalities.

The critical question is not so much why they rely on abductive reasoning but why their simplest and most likely explanation by default leads to a suspicion transaction report. Other explanatory hypotheses might have been conceived, but, for some reasons, they are not or they are dismissed in favour of suspicion. These reasons first and foremost relate to the occupational ‘culture of suspicion’ at the core of anti-money laundering and counterterrorist financing compliance. As part of their raison d’être and organizational position within banks, chief anti-money laundering officers and related employees aim to protect their institution against “the risk of financial and reputational losses” in relation to (anti)money laundering and (counter)terrorism financing (Power, 2004: 58; Van Duyne et al., 2016). It is widely shown in the literature how banks have massively invested in defendable compliance to protect themselves from regulators rather than from criminals (Gelemerova, 2009; Favarel-Garrigues et al., 2011; Hibou, 2015; Amicelle In press). The primacy of ‘institutional risks’ with a view to avoiding blame, shame and sanctions has direct consequences for suspicion and reporting, with well-known tendency of defensive reporting (ibid.). Harvey and Lau have summed up this tendency among banks “to report everything that might appear merely unusual in order to achieve the regulatory equivalent of ‘covering their backs”’ (2008: 61).

In Canada’s banking industry, the phenomenon of defensive reporting is recognized but to better put it to the past tense. “Back in 2002, it was defensive because we weren’t clear on what the triggers were, you know, indicators. So, we were floundering a bit, trying to find some of those. It was lot more defensive” (Interview within a bank, 2015). While interviewees in banks converge to say that current reporting practices are less defensive than before, their interviews indicate at least that defensive reporting is subtler than before. It is gradually restricted to the 'does not make sense' type of situation. To put it clearly, we do not argue that a defensive report may never prove to be intelligence-relevant per se. We rather argue that the interplay of security-related legal obligations, banks corporate interests and organizational position of compliance resources favours the reduction of suspicion to a mere hunch, that is a "presumption which does not emerge from arguments, but is rather caused by environmental factors which affect almost unconsciously the mental atmosphere and may become influential in decision-making" (Palmieri and Rigotti, 2014: 303). Ultimately, Fintrac officials are the ones who face the challenge of controlling the quality of suspicion to draw the blurred line between intelligence-relevant and non-relevant reporting.

2.2) *Quality Control of Suspicion*

In accordance with its mandate, Canada's financial intelligence unit is engaging in ensuring compliance of reporting entities. Three chronological phases can be identified about the evolutive power relationships between Canada's financial intelligence unit and reporting entities. From 2001 to 2008, Fintrac officials started with a public relations exercise to raise awareness about the stated importance of legal obligations against money laundering and terrorist financing. From 2008 to 2013, they enforced examinations with a focus on 'technical compliance', including five elements such as the appointment of a compliance officer (Fintrac 2017). Since 2014, they have insisted on a shift towards "compliance for intelligence" to set a new "operating paradigm" with higher expectations in relation to the quality of financial transactions reports (Fintrac 2016c). As recalled by a Fintrac official, "they have beautifully packaged compliance regimes. The highest paid consultants would write them. They would give them to the banks who would hand them to us. They are beautiful but we want to see how it is implemented. And the other thing we are doing is we are looking for suspicious transactions too" (Interview within Fintrac, 2015). In practice, banks' compliance for intelligence is partly examined through the dual quality control of suspicious transaction reports.

'Compliance for intelligence' in practice

First of all, quality control of suspicion is dedicated to missing reports, i.e. internal alerts which must have been submitted to Fintrac. The reasons for not making a report based on an internal alert have to be documented. "Yes, you have to write a report and it cannot just be 'not suspicious'. It has to be why it is not suspicious. It takes time, the explanation in the system and the system itself...and reviewing the transaction...it just takes a lot of time no matter how much you try to...reduce the time" (Interview within a bank, 2015). During compliance examinations, Fintrac auditors request access to banks' internal inquiries and information about alerts that have not led to suspicious transaction reports. As declared by a Fintrac official, "The big challenge is to find non-reported STRs because this will show compliance loopholes […]" (Interview within Fintrac, 2015). Once again, the challenge lies in knowing where to draw the line between irrelevant alerts and reportable abnormalities.

At first glance, Fintrac auditors need to answer a very plain and simple question: Is the decision not to make a report correct or not? Despite appearances, they are not necessarily, however, in a position of strength to answer this question. The reporting system as a whole has been built and promoted on the premise that banks are the ones best placed to know whether a transaction is suspicious or not. Although banking actors used to complain to be in the frontline, they also play with this situation as a resource in the argumentative battle about suspicion. As a legally poorly defined notion, suspicion ultimately refers to "an argumentative move" (Palmieri and Rigotti 2014). A compliance officer illustrated this point: "One must of course have reasonable grounds to suspect. It is clear but we can challenge this because a reasonable ground for someone is not a reasonable ground for someone else. Sometimes we 'fight' this with Fintrac" (Interview within a bank, 2016). If nothing is inherently suspicious (Norris, 2003), the qualification of a conduct as suspicious ultimately remains a matter of argument.

Consequently, the main question for compliance examinations is rather: Are bank representatives able to explain and justify their decision? Fintrac auditors try as much as possible to rely on 'objective' indicators for ensuring a re-balanced interplay of the forces involved in the argumentative battle. As exemplified by a Fintrac official: "Here is a transaction that a person has come in several times in a week, and have deposited 20 000$ in cash. And it says that he is unemployed. What's going on here? Tell me Mister compliance officers. Why? Who is this person? So then the compliance officers would say yes. The person is unemployed and he received an inheritance. They can explain it. Other times they are silent. Part of your indicators says that if the person's income or employment does not match the transactions in their account, then it is reportable. Again, why wasn't this reported? So I always bring it back to the policies and procedures" (Interview within Fintrac, 2015). Along these lines, one bank has been sanctioned because of reporting failures since the creation of Fintrac in 2000. Violation of the law was evidenced—and admitted—based on the unjustified incoherence between bank's reporting procedures and bank's reporting practices, including failure to report a case of 'transferred suspicion' (Cribb et al., 2016). This is a textbook case of 'obvious' non-compliance demonstrated in the light of clearly objectified criteria but it is worth noting that this is also the only one ever for banks.

Secondly, quality control of suspicion is also dedicated to false positives, i.e. reports which should not have been submitted to Fintrac. "We call them "safe heavens", STRs [suspicious transaction reports] that are not STRs. One of the things that we look at when they send an STR is the justification, "why". What are their motives? There was a time when we literally received reports about 500$ cash deposit in an ATM. I do not want this STR unless you tell me that guy is the local drug dealer and that's what he does. We spend a lot of time during the examination to understand what they write in the G part [the argumentative section—free text in the reporting form]. What is in the G part? What are your indicators for leading to your suspicion? Because I do not want useless STRs for my analysts" (Interview within Fintrac, 2015). The issue of safe heavens overlaps with the phenomenon of defensive reporting. Once again, the distinction between relevant/justified and non-relevant/purely defensive reporting is ultimately a matter of discussion between the audited and the auditor. This indirectly highlights the magnitude, if not the impossibility, of the challenge of assessing suspicion quality without knowing the full consequences of financial intelligence-related investigations that are only episodically followed up. Moreover, the distinction is also discussed within Fintrac. According to the intelligence perspective from which more data is always the best security option, certain officials argue that the very same report can be seen as defensive for the moment but can be potentially relevant for the future.

Taking this argument to the extreme would be a call for the end of another distinction, the one between internal alerts and suspicious transaction reports. This is rather a debate among security-oriented institutions than among banking actors. "Everyone has a system that looks for unusual activities. Let's say, within your institution, you process that activity and you have 10 000 alerts a month, 10 000 things that are may be suspicious. Let's say, for the sake of argument, that's 10 000 STRs [suspicious transactions reports] that you would file. The human capita that will be needed to file 10 000, and then to file in a timely fashion to meet expectations would be huge. And then, if you think of the flip side of that, if we file 10 000, and the other four large banks, they file 10 000 every month, that means law enforcement now has 50 000 STRs coming at them a month. How do they work those? How do they say which are the good ones and which aren't? Well not which are the good one but which are the ones really should be investigated? Let's face it, the STRs are supposed to help benefit law enforcement so that they can conduct the investigation" (interview within a bank, 2015). In addition to the argument of security effectiveness, banks reject the idea to report every alert of abnormality because of financial costs. A report must be filed within 30 days after the date a transaction or a set of transactions is formally considered as suspicious. The reporting form includes over 130 fields and takes from one to two days to be completed, sometimes more. For instance, a bank had to report over 1,700 transactions at the same time in relation to one case while one reporting form allows a maximum of 99 transactions. Systematic investigation is less time-consuming and expensive than reporting everything for financial institutions with tens of thousands, hundreds of thousands or millions of alerts annually. In other words, the ultimate defensive reporting regulator is money.

Although the quality control of suspicion is both focused on 'false-positives' and 'false-negatives' reports, the pressure is first and foremost related to the latter, i.e. the missing reports. Fintrac penalties for non-compliance reflect this trend. They only include sanctions for 'failure to report suspicious transactions' (up to $2 million and five-year imprisonment). From banks' perspective, defensive over-reporting is de facto the strategy of choice to 'cover their backs'. The daily costs of reporting practices prevent banks to report everything but over-reporting remains far less problematic than under-reporting in terms of reputational risk and related-financial consequences.

CONCLUSION

A culture of suspicion can be simply conceptualised as a climate lacking in trust, often indicated by a reluctance of people to enter into any relations with others without intensely monitoring the risks of failure. (Chan, 2008: 234)

The culture of suspicion is intended to be an occupational one in the name of the fight against "the chameleon threat of dirty money" (Mitsilegas 2003). To paraphrase Ragazzi about police officers (2017: 227), if bank employees—from the counter staff to the operational units—are not suspicious to others, they are not doing their job properly. All of them have to be involved, to varying degrees, in the production process of suspicion from which the final product is the report to State authorities. The paper questions three key moments of this process at work in many more law enforcement and counterterrorism areas than the policing of financial activities.

First of all, suspicious activity reporting relies on the dynamic interplay of surveillance with the construction of risk and (ab)normality. On the one hand, risk-scoring is the frequency modulator of surveillance to decide where and who to look more intensively. On the other hand, the production of suspicion yokes to the infralegal distribution of normal and abnormal conduct. For instance, indicators mainly refer to small singularities that do not constitute legal transgressions as such. Most of the time, they are well below the legal order, but they can be associated with the possibility of a transgression according to their designers and end-users. The definition of (ab)normality is the trigger component for surveillance to decide what to look for. Alert systems depend to a large extent on the combination settings of surveillance, risk and (ab)normality.

Secondly, suspicious activity reporting relies on the investigation of alerts as enigmas that shed light on situations that disturb a set of expectations about normality. In principle, the resolution of enigmas lies in the subtle correlation made between abnormal and suspicious rather the crude opposition of normality and suspicion. In practice, Canada's configuration of financial policing shows that such a resolution blurs the lines between suspicion-based reporting and abnormality-based reporting. By contrast to official guidelines, suspicious transaction reports are not only the result of reasonable grounds to suspect that financial transactions are related to the commission or the attempted commission of a money laundering offence or a terrorist activity offence. In addition to the so-called obvious cases of suspicious conduct, suspicion is produced and report is filed when the conduct under investigation 'does not make sense' according to the financial policing agents.

Thirdly and lastly, suspicious activity reporting relies on an ongoing quality control. Here, suspicion appears as a boundary object that is double-edged for state authorities. On the one hand, its interpretive flexibility allows state actors from security-oriented institutions to work with social actors from non-security-oriented institutions without consensus. Security-oriented institutions may even try to benefit from the unease that stems from the interpretive flexibility to increase the daily involvement of potential informers. Along these lines, Fintrac indicates that, "as a general guide, a transaction may be connected to money laundering or terrorist activity financing when you think that it (or a group of transactions) raises questions or gives rise to discomfort, apprehension or mistrust" (Fintrac, 2017). On the other hand, the interpretive flexibility makes it impossible to mark out the exact contours of suspicion and the intrinsic value of the information supplied. "A lot of work is done to improve the quality of suspicious transaction reports and at the same time to regulate the levels of reporting to say you know that is suspicious, but it is a tough thing because suspicion is in the eye of...well it's not, there's a legal definition, but it is very much in the eye of the beholder" (Interview within Fintrac, 2015). Suspicion is not a question of discovery but a question of interpretation. The prevalence of interpretive statement over cold facts transforms the quality control of suspicious activity reporting into an argumentative battle between State security-oriented institutions and their designated 'eyes and ears'.

References

Alpert, G. P., MacDonald, J. M. and Dunham, R. G. (2005), 'Police Suspicion and Discretionary Decision Making During Citizen Stops', *Criminology*, 43: 407–34.

Amicelle, A. (2011), 'Towards a "New" Political Anatomy of Financial Surveillance', *Security Dialogue*, 42: 161–78.

Amicelle, A. (In press), 'Policing Through Misunderstanding: Insights From the Configuration of Financial Policing', *Crime, Law and Social Change*.

Amoore, L. and De Goede, M. (eds) (2008), *Risk and the War on Terror*. Routledge.

Amoore, L. and De Goede, M. (2008). Transactions after 9/11: the banal face of the preemptive strike. *Transactions*, 33 (2) : 173–185.

Andrejevic, M. (2006), 'The Work of Watching One Another: Lateral Surveillance, Risk and Governance', *Surveillance and Society*, 2: 479–97.

Bauman, Z., Bigo, D., Esteves, P., Guild, E., Jabri, V., Lyon, D. and Walker, R. J. B. (2014), ‘After Snowden: Rethinking the Impact of Surveillance’, *International Political Sociology*, 8: 121–44.

Becker, H. (1998), *Tricks of the Trade: How to Think About Your Research While You're Doing It*. Chicago University Press.

Bergström, M., Helgesson, K. S. and Mörth, U. (2011), ‘A New Role for For-Profit Actors? The Case of Anti-money Laundering and Risk Management’, *Journal of Common Market Studies*, 9: 1043–64.

Bigo, D. and Guittet, E-P. (2011), ‘Northern Ireland as Metaphor: Exception, Suspicion and Radicalization in the “War on Terror”’, *Security Dialogue*, 42: 483–98.

Boltanski, L. (2011), *E□nigmes et complots: une enquête a□ propos d'enquêtes*. Gallimard Gallimard, NRF essais.

Bossio, D. (2005), ‘Be Alert, Not Alarmed: Governmental Communication of Risk in an Era of Insecurity’, available online at http://www.anzca.net/documents/2005-conf-papers/247-be-alert-not-alarmed-governmental-communication-of-risk-in-an-era-of-insecurity-1/file.html.

Cardon, D. (2015), *À quoi rêvent les algorithmes ?* Paris : Éditions du seuil.

Chan, J. (2007), ‘Dangerous art and suspicious packages’, Law Text Culture, 11: 51–69.

Chan, J. (2008), ‘The New Lateral Surveillance and a Culture of Suspicion’, in M. Deflem, eds., Surveillance and Governance: Crime Control and Beyond, Vol. 10. Sociology of Crime, Law and Deviance, Emerald/JAI Press.

Conroy, J. (2015), *Global AML vendor evaluation : Managing rapidly escalating risk*. AITE.
Cribb, R., Oved, M. C. and De Souza, M. (2016), ‘Canadian Bank Failed to Report 1,200 Suspicious Transactions’, *The Toronto Star*, 22 December.

De Goede, M. (2007), ‘Underground Money’, *Cultural Critique*, 65: 140–63.

De Goede, M. (2008), 'Risk, Preemption and Exception in the War on Terrorist Financing', in L. Amoore and M. de Goede, eds, *Risk and the War on Terror*, 97–111. Routledge.

De Goede, M. and Sullivan, G. (2016), 'The Politics of Security Lists', *Environment and Planning D: Society & Space*, 34: 67–88.

Dewey J. (1938), *Logic : The theory of inquiry*. New York : Holt.

Department of Finance Canada (2015), *Assessment of Inherent Risks of Money Laundering and Terrorist Financing in Canada*. Department of Finance Canada.

Dixon, D., Bottomley, A. K., Coleman, C., Gill, M. and Wall, D. (1989), 'Reality and Rules in the Construction and Regulation of Police Suspicion', *International Journal of the Sociology of Law*, 17: 185–206.

Durkheim, E. (1988) (1895), *Les règles de la méthode sociologique*. Paris : Flammarion.

Douven, I. (2016), 'Abduction', in E. N. Zalta, ed., *The Stanford Encyclopedia of Philosophy*, Winter 2016 edn, available online at https://plato.stanford.edu/entries/abduction/.

Ericson, R. (1982), *Reproducing Order: A Study of Police Patrol Work*. University of Toronto Press.

Ericson, D. (2007), *Crime in an Insecure World*. Polity Press.

Fagan, J. and Geller, A. (2015), 'Following the Script: Narratives of Suspicion in Terry Stops in Street Policing', *University of Chicago Law Review*, 82: 51–88.

FATF (2004), *The Financial War on Terrorism: A Guide by the Financial Action Task Force*.

FATF. FATF (2016), *Mutual Evaluation Report of Canada*. FATF.

Favarel-Garrigues G., Godefroy, T. and Lascoumes, P. (2008), 'Sentinels in the Banking Industry: Private Actors and the Fight Against Money Laundering in France', *British Journal of Criminology*, 48: 1–19.

Favarel-Garrigues, G., Godefroy, T. and Lascoumes, P. (2011), 'Reluctant Partners? Banks in the Fight Against Money Laundering and Terrorism Financing in France', *Security Dialogue*, 42: 179–96.

Favarel-Garrigues, G., Godefroy, T. and Lascoumes, P. (2012). Tools and securitization: the instrumentation of AML/CTF policies in French banks, In Svedberg Helgesson, K. and Mörth, U. (eds.). *Securitization, accountability and risk management: Transforming the public security domain*. New York : Routledge, PRIO New Security Studies.

Fintrac (2016a), *Transactions that Must Be Reported*. Fintrac.

Fintrac (2016b), *Who We Are*. Fintrac.

Fintrac (2016c), *FINTRAC Annual Report: Results in the Fight Against Money Laundering and Terrorism Financing*. Fintrac.

Fintrac (2017), *FINTRAC Guidelines. Guideline 2: Suspicious Transactions*. Fintrac.

Foucault, M. (2003), *Abnormal: Lectures at the Colle□ge de France, 1974–1975*. Verso.

Gelemerova, L. (2009), 'On the Frontline Against Money-Laundering: The Regulatory Minefield', *Crime, Law and Social Change*, 52: 33–55.

Gold, M. and Levi, M. (1994), *Money Laundering in the UK: An Appraisal of Suspicion-Based Reporting*. The Police Foundation and University of Wales.

Guittet, E.-P. (2015), 'How Generalised Suspicion Destroys Society', *Open Democracy*, available online at https://www.opendemocracy.net/can-europe-make-it/emmanuelpierre-guittet/how-generalised-suspicion-destroys-society.

Guittet, E.-P. and Brion, F. (2017), 'The New Age of Suspicion', in E. Eklund, E.-P. Guittet and A. Zevnik, eds, *Politics of Anxiety*. 79–99. Rowman & Littlefield.

Harvey, J. and Lau, S. F. (2008), ‘Crime-Money, Reputation and Reporting’, *Crime, Law and Social Change*, 52: 57–72.

Helgesson, K. S. and Mörth, U. (2016), ‘Involuntary Public Policy-Making by For-Profit Professionals: European Lawyers on Anti-money Laundering and Terrorism Financing’, *Journal of Common Market Studies*, 54: 1216–32.

Hibou, B. (2015), *The Bureaucratization of the World in the Neoliberal Era*. Palgrave Macmillan.

Hickman, M. J., Lyn Thomas, H. C. N. and Silvestri, S. (2012), ‘Social Cohesion and the Notion of “Suspect Communities”’, *Critical Studies on Terrorism*, 5: 89–106.

Huysmans, J. (2014), *Security Unbound: Enacting Democratic Limits*. Routledge.

Jarvis, L. and Lister, M. (2015), *Anti-terrorism, Citizenship and Security*. Manchester University Press.

JMLSG (2017), *Prevention of Money Laundering and Terrorist Financing: Guidance for the UK Financial Sector*. JMLSG.

Larsen, M. and Piche□, J. (2009), ‘Public Vigilance Campaigns and Participatory Surveillance After 11 September 2001’, in S. P. Hier and J. Greenberg, eds, *Surveillance: Power, Problems and Politics*. UBC Press.

Levi, M. (1991), ‘*Pecunia non olet*: Cleansing the Money-Launderers from the Temple’, *Crime, Law and Social Change*, 16: 217–302.

Levi, M. (2005), ‘Money Laundering and Regulatory Policies’, in E. Savona, ed., *Responding to Money Laundering: International Perspectives*, 257–78. Taylor & Francis.

Levi, M. (2010), ‘Combating the Financing of Terrorism: A History and Assessment of the Control of “Threat Finance”’, *British Journal of Criminology*, 50: 650–69. Lyon, D. (2003), *Surveillance After September 11*. Polity Press.

Lofland, L. H. (1973). *A World of Strangers: Order and Action in Urban Public Space*. New York: Basic Books.

Lyon, D., Haggerty, K. and Ball, K. (2012), 'Introducing Surveillance Studies', in K. Ball, K. Haggerty and D. Lyon, eds, *Routledge Handbook of Surveillance Studies*, 1–12. Routledge.

Mitsilegas, V. (2003), 'Countering the Chameleon Threat of Dirty Money', in A. Edwards and P.Gill, eds, *Transnational Organized Crime: Perspectives on Global Security*, 195–211. Routledge.

Monahan, T. (2010), *Surveillance in the Time of Insecurity*. Rutgers University Press.

Murakami Wood, D. (2012), 'Globalization and Surveillance', in K. Ball, K. Haggerty and D. Lyon, eds, *Routledge Handbook of Surveillance Studies*, 333–42. Routledge.

Mythen, G. and Walklate, S. (2016), 'Counterterrorism and the Reconstruction of (In)security: Divisions, Dualisms, Duplicities', *British Journal of Criminology*, 56: 1107–24.

Naylor, R. T. (1999), 'Washout: A Critique of Follow-the-Money Methods in Crime Control Policy', *Crime, Law and Social Change*, 32: 1–58.

Norris, C. (2003), 'From Personal to Digital: CCTV, the Panopticon, and the Technological Mediation of Suspicion and Social Control', in D. Lyon, ed., *Surveillance as Social Sorting: Privacy, Risk, and Digital Discrimination*, 249–81. Routledge.

Nice Actimize (2015). *Suspicious activity monitoring. Anti-money laundering solutions*, available online at : http://www.niceactimize.com/Lists/Brochures/AML_Brochure_SuspiciousActivityMonitoring.pdf

Palmieri, R. and Rigotti, E. (2014), 'Suspicion as an Argumentative Move. Semantic Analysis of a Pivotal Concept in Banks' *Anti-money Laundering* Argumentative Activities', *Journal of Argumentation in Context*, 3: 287–321.

Pantazis, C. and Pemberton, S. (2009), 'From the "Old" to the "New" Suspect Community: Examining the Impacts of Recent UK Counter-Terrorist Legislation', *British Journal of Criminology*, 49: 646–66.

Patel, T. (2012), 'Surveillance, Suspicion and Stigma: Brown Bodies in a Terror-Panic Climate', *Surveillance & Society*, 10: 215–34.

Pinson, G. and Sala Pala, V. (2007), 'Peut-on vraiment se passer de l'entretien en sociologie de l'action publique?', *Revue française de science politique*, 57: 555–97.

Power, M. (2004), 'The Risk Management of Everything', *The Journal of Risk Finance*, 5: 58–65.

Protiviti (2013). *Views on AML monitoring systems. From system selection to effective governance*, available online at : https://www.protiviti.com/sites/default/files/united_states/insights/views-on-aml-transaction-monitoring-systems-protiviti-uk.pdf
Ragazzi, F. (2016), 'Suspect Community or Suspect Category? Counter-Terrorism as "Policed Multiculturalism"', *Journal of Ethnic and Migration Studies*, 42: 724–41.

Ragazzi, F. (2017), 'Countering Terrorism and Radicalisation: Securitising Social Policy?', *Critical Social Policy*, 37: 163–79.

Regan, P. M., Monaha, T. and Craven, K. (2015), 'Constructing the Suspicious: Data Production, Circulation, and Interpretation by DHS Fusion Centers', *Administration & Society*, 47: 740–62.

Reeves, J. (2012), 'If You See Something, Say Something: Lateral Surveillance and the Uses of Responsibility', *Surveillance & Society*, 10: 235–48.

Reuter, P. and Truman, E. (2004), *Chasing Dirty Money: The Fight Against Money Laundering*. Institute for International Economics.

Ritchie, M. (2015), 'Feeling for the State: Affective Labor and Anti-terrorism Training in US Hotels', *Communication and Critical/Cultural Studies*, 12: 179–97.

Ruppert, E. (2012). The Governmental Topologies of Database Devices. *Theory, Culture and Society*, 29(4-5) : 116-136.

SAS (2015). *Transaction monitoring : To segment or not? One size never fits all, but a dynamic segmentation strategy does*, available at : https://www.sas.com/fr_ca/insights/articles/risk-fraud/transaction-monitoring-dynamic-segmentation.html

Shamir, R. (2005), 'Without Borders? Notes on Globalization as a Mobility Regime', *Sociological Theory*, 23: 197–217.

Sharman, J. (2011), *The Money Laundry: Regulating Criminal Finance in the Global Economy*. Cornell University Press.

Stalcup, M. (2015), 'Policing Uncertainty: On Suspicious Activity Reporting', in L. Saminian-Darash and P. Rabinow, eds, *Modes of Uncertainty: Anthropological Cases*, 69–87. Chicago University Press.

Taylor, E. (2012), 'The Rise of the Surveillance School', in K. Ball, K. Haggerty and D. Lyon, eds, *Routledge Handbook of Surveillance Studies*, 225–32. Routledge.

van Duyne, P., Harvey, J. and Gelemerova, L. (2016), 'The Monty Python Flying Circus of Money Laundering and the Question of Proportionality', in G. A. Antonopoulos, ed., *Illegal Entrepreneurship, Organized Crime and Social Control: Essays in Honour of Professor Dick Hobbs*, 161–87. Springer.

Vaughan-Williams, N. (2008), 'Borderwork Beyond Inside/Outside? Frontex, the Citizen– Detective and the War on Terror', *Space and Polity*, 12: 63–79.