The Annual Review of Interdisciplinary Justice Research

Volume 3, Fall 2012

Edited by
Steven Kohm
The University of Winnipeg
Centre for Interdisciplinary Justice Studies (CIJS)
ISSN 1925-2420

Policing Money Laundering and Terrorist Financing: The Identification and Reporting of Suspicious Transactions

Vanessa Iafolla, Centre for Criminology and Sociolegal Studies
University of Toronto[1]

Introduction

It is held in banking as a truism that the terrorist attacks of September 11, 2011, 'changed everything'. While Canada, like many other advanced liberal democracies, had already enacted anti-money laundering legislation, 9/11 pushed money laundering and terrorism financing to the forefront of Canadian politics and policy. Since then, activities that could be related to terrorism—including financial transactions—have come under increasing scrutiny from both individuals employed in the public and private sectors, and financial transactions taking place in part or in whole in Canada are subject to increased scrutiny at the behest of Canadian anti-terrorism laws.

In the wake of the terrorist attacks of that day, the financial services sector was identified as susceptible to abuse by money launderers and financiers of terrorism (Murphy, 2003), and Canada rushed to amend its laws relating to the policing of financial activities (Daniels, 2001). Some of these

1. This research was supported by the Social Sciences and Humanities Research Council of Canada. An earlier version of this paper was presented at the Centre for Interdisciplinary Justice Studies. The author thanks Anna Morrison and James A. Morrison for their support. Direct correspondence to Vanessa Iafolla, Centre for Criminology and Sociolegal Studies, University of Toronto, 14 Queens Park Cres. W., Toronto ON, M5S 3K9, or vanessa.iafolla@utoronto.ca.

amendments became part of the *Proceeds of Crime (Money Laundering) and Terrorism Financing Act* (2000) (PCMLTFA), which, for the first time, introduced the financing of terrorism as an offence in Canadian law, and which expanded the duties of employees in identified industries that deal with financial transactions, such as banking, to report any transactions they understand to be 'suspicious' to Fintrac, the Financial Transactions Reporting and Analysis Center of Canada (Fintrac 2012b). Fintrac analyses intelligence from multiple sources and discloses information to government agencies, including the RCMP and CSIS (Fintrac 2010). According to the PCMLTFA, employees in industries identified by the legislation must report to Fintrac any and all transactions with a value of less than $10,000 that appear "suspicious" (Fintrac, 2011c). The law does not set out specifically what it holds to be suspicious, instead stating that suspect transactions must be identified according to the norms of each industry (Fintrac, 2011). Beyond this instruction, however, little is known about what 'suspicious' actually means or how 'suspiciousness' is operationalized. Likewise, the specific factors employees consider when deciding to submit a report of suspicion are unclear, and little is known about the effects that such surveillance may have for bank clients.

This paper examines the application of the *Proceeds of Crime (Money Laundering) and Terrorist Financing Act* (PCMLTFA) in the financial services sector. Specifically, it looks at the ways bank employees discharge their legal duties to report suspicious transactions and inquires into the implications of identifying suspicious transactions for clients, who under the law cannot know that their transactions have been reported (Fintrac 2012a). Under the PCMLTFA, employees are to determine 'suspiciousness' by determining whether a client's transaction deviates from industry norms. It is up to individual employees to decide whether a transaction is atypical: to that end, what is suspicious is not only to be determined in accordance with industry norms, but may be decided on a case-by-case basis. In light of this broad yet subjective man-

date to report, it is important to understand what motivates employees to make reports of suspicion.

Background

While there have been amendments to Canada's proceeds of crime legislation since its enactment in 1991, none have had quite the impact of those in Bill C-36 (2001). The Bill, created as a swift response to the terrorist attacks of September 11, 2001, "was designed to enhance the federal government's capacity to protect Canada from terrorist threats, as well as allowing it to contribute more effectively to international efforts aimed at combating global terrorism" (Daniels, 2001, p. 3). Bill C-36 (2001), enacted that year in part as the *Anti-terrorism Act*, sought to amend ten statutes and to ratify UN Conventions related to the suppression of the financing of terrorism and the suppression of terrorist bombings (Roach, 2003; Roach, 2001). Of the many projected adverse impacts to Canadian civil liberties and freedoms, issues regarding the regulation of financial transactions, or, more simply put, issues related to how the detection of terrorist financing would be carried out, raised sharp criticism from members of the academic community and from civil society: less than two months following 9/11, Canadian academics convened at the University of Toronto Faculty of Law to discuss the then-proposed omnibus anti-terrorism legislation. This conference, which later resulted in a collection of scholarly essays (Daniels, Macklem, & Roach, 2001), was one of many manifestations of collective criticism from the academic community. Academics, community agencies, and private citizens formed ad hoc groups, signing open letters to Parliament (Canadian Peace Alliance, 2001) and making submissions to the Senate Special Committee on Bill C-36 (Iafolla, 2011). In addition to creating specific provisions to the *Anti-terrorism Act* that made it illegal to facilitate terrorism—a noble end, if problematic in scope and application (Davis, 2001; Duff, 2001)—the legislation also required all individuals working in identified industries to report activities deemed suspicious and in some way related to the financing of terrorism (Fintrac 2012b).

Canada's proceeds of crime legislation at the time required all individuals working in industries dealing with cash transactions—including banking, real estate, insurance, and casinos, among others (Fintrac 2012b)—to report transactions that in some way deviated from standard transactions in their industries, and reporting was specifically limited to money laundering (Beare & Schneider, 2007). The 2001 amendments to Canada's anti-money laundering legislation put terrorist financing at the forefront, publicly underscoring Canada's "international commitments to participate in the fight against transnational crime, particularly money laundering, and the fight against terrorist activity" (s.3c). However, the law refrained from providing much in the way of guidance beyond a directive to report "every financial transaction that occurs or that is attempted in the course of their activities and in respect of which there are reasonable grounds to suspect" (s.7) attempted or actual money laundering or terrorist financing.

The 'reasonable grounds' upon which an individual should submit a report of suspicion—the Suspicious Transaction Report (STR)—are not elaborated upon in the legislation, nor are they clearly evinced by regulators. The law does identify particular transactions that must be reported, such as cash deposit transactions at or above $10,000.00 (Fintrac, 2012a). However, and unlike 'threshold' transactions where the dollar value of the transaction provides a clear rule for reporting, any transaction, regardless of its value, must be reported if the employee processing it thinks the transaction is in some way suspicious. Here, the law offloads the process of determining what is suspicious and how suspicious transactions should be detected onto the private sector.

Policing Financial Transactions

Academic discourse has thoroughly documented the trend in modernity toward embedding policing functions in private settings: embedded security has been identified in a multi-

tude of settings in which economic or property interests require protection: sites as disparate as Disney World (Shearing & Stenning, 1984), retail banks (Iafolla, 2004), airports (Rigakos & Greener, 2000), and private neighbourhoods (Brown & Lippert, 2007) all rely on elements of private security, in part or in whole, to secure their interests. Security in some areas is increasingly pluralized. For example, Rigakos & Greener (2000) demonstrate that multiple policing bodies—state and non-state—operate within the space of Lester B. Pearson Airport. The pluralisation of policing is a feature of late modernity, contiguous with the trend toward downloading policing from the state's auspices to the private sector (Osborne & Gaebler, 1992). These intersecting spaces of private-public interest, wherein access to the public is encouraged (particularly for reasons of commerce or profit-building) yet security is provided according to the mandate of the private property owner, are described variously described in the scholarly literature as pockets of "nodal governance" (Shearing and Wood 2003), or of hybrid policing (Brodeur, 2010; Johnston, 2000). These are loci where private and public policing functions not only may overlap and interface, but wherein public policing functions may at least in part be performed by private agents.

The features of 'private' and 'public' policing have been closely examined in academic scholarship, however, what is less understood is the way in which private policing agents, or private individuals, may be legally mandated to engage in a policing function on behalf of the state. Downloading the detection of a particular crime or regulatory infraction almost entirely to the private sector is not unprecedented (cf: Ayling & Grabosky, 2006). What is novel about the case of third-party policing in this context is that frontline bank staff are simultaneously responsible for protecting the profit-building interests of their employers (Iafolla, 2004) while conducting an important public security function, all of which takes place in the context of employment activities that are not security-related. Employees must balance two competing concerns and logics, simultaneously and routinely

undertaking private *and* public policing functions in the course of their jobs.

Further, in the case of anti-money laundering and anti-terrorist financing initiatives, the PCMLTFA almost entirely removes public policing bodies from the initial stages of detection and investigation. Certainly, there are government agencies or individuals employed by the government responsibilized into disclosing reports to Fintrac. For example, "agents of the Crown licensed to sell money orders" must report suspicious financial transactions (Fintrac, 2011a). Still, the list of persons and entities identified by the legislation is largely comprised of private, for-profit enterprises that are not funded from public coffers, including Schedule II banks, loan and trust companies, and businesses that involve the remittance of funds (Fintrac, 2012c). The focus of the law in this area is sharpest on those areas beyond government, and traditional policing bodies are generally not involved in policing these sorts of financial crimes until after STRs have been vetted by Fintrac. As well, according to Fintrac, "'[r]easonable grounds to suspect' is determined by what is reasonable in your circumstances, including normal business practices and systems within your industry" (Fintrac, 2010b). Constructing reasonable grounds for suspicion in this way—as an individualized exercise of discretion based on an employee's understanding of industry standards—takes this element of investigation out of the hands of public policing agencies.

Transforming a policing function into one that is almost entirely the responsibility of the private sector—particularly with such scant instructions—presents challenges, particularly given the scope of activities, size of the entities covered under the legislation, and the number of individuals working in industries identified by the legislation. Canadian retail banking alone is enormous: according to the Canadian Banker's Association, more than 96% of Canadians have a bank account (Fintrac, 2012a). The financial activities of virtually every person in Canada may be subject to scrutiny, as financial institutions examine individual bank accounts

for suspicious activity on a regular basis. Although in-branch banking is no longer the preferred choice of many Canadians, as, according to the Canadian Bankers Association (CBA) only 23% of Canadians use in-branch banking as their primary method of accessing financial services (CBA 2012), the potential for Canadians to transact with larger amounts of cash in branch makes in-branch employees an important source of intelligence for financial institutions, as there are 6,175 bank branches of 75 different banks across Canada (CBA, 2012). One need only visit a branch once to become the subject of this form of surveillance. The potential reach of the policing apparatus into the financial lives of Canadians is vast, yet, little is known about how this particular type of policing occurs, nor what the impact on clients whose financial dealings are identified as risky might be.

In financial institutions, this apparatus includes an internal process to cope with the volume of transactions to inspect for irregularities. Among the various techniques of governance developed to facilitate the detection efforts of financial institutions is the Unusual Transaction Report (UTR). The UTR is an internal precursor to the STR that is required of all responsibilized industries and individuals. Financial institutions have developed the UTR for two reasons. Firstly, the UTR exists to fulfil the legal obligation put upon employees, including those in retail banking, to identify transactions that deviate from the norm (Bank Manual[2]) without directly submitting a report to Fintrac. A UTR generated by retail employees is but one of a number of intelligence tools that may eventually form an STR (Bank Manual). Secondly, the UTR helps streamline the reporting process for financial institutions. Prior to submitting STRs to Fintrac, financial institutions will collate and analyse UTRs and other reports of irregular financial activity internally (Bank Manual). Where the activity appears suspicious, the financial institution will

2. Due to the research access agreement, of which the anonymity of the bank was a condition, this research may cite information from internal manuals and other data, but cannot cite the author, publisher, or titles of internal publications. To honour that agreement, internal publications such as bank manuals, where cited, will therefore not be listed in the references of this paper.

send the information as an STR to Fintrac (Bank Manual). Otherwise, the information is deemed 'not suspicious' and no further action is taken (Bank Manual). From the perspective of the financial institution, the UTR is a crucial part of the reporting process. It is the sole vehicle through which retail bank employees may make a report of suspicion (Bank Manual), and in many instances may be the initial report that identifies a suspicious transaction, or may provide intelligence for a larger investigation (Bank Manual).

The financial intelligence gleaned from UTRs is qualitatively different from that generated by data mining and other analytics techniques[3]. Data mining and similar analytics techniques generate information based on algorithms that identify particular patterns of activity (Zdanowicz 2004; Levi 2002). UTRs differ in that the intelligence generated by employees contains information related to customer demeanour and behaviour, including such information as the kinds of clothing worn by the client, employee perceptions of the client's demeanour and behaviour, the smell of the money brought in for deposits, and the condition the bills are in (UTR forms). Thus, UTRs are the only sort of financial intelligence in which the client's physical presence may influence the teller's decision to report a transaction. The decision to submit a report of suspicion is left to the individual employee, and although reports should be grounded in industry norms, there are myriad reasons a transaction might appear unusual or suspicious to the individual conducting it, including those beyond the stated objectives of the PCMLTFA.

Methodology

This research used a qualitative methodology. Data collection took place in one of Canada's largest financial institutions: 40 interviews were conducted with employees at randomly selected bank branches in the City of Toronto. Access to bank manuals was a key component of this research, as bank poli-

3 "Analytics" refers to the collective techniques of governance that identify particular kinds of risky transactions through algorithmic analysis.

cies and procedures to be followed with regard to reporting unusual financial transactions, including banking best practices, were derived from official narratives on this topic. Training manuals, training programs, and internal publications on 'red flags' for money laundering and terrorist financing comprise the official discourse on detecting unusual financial activity, and according to the bank should frame the decision to report suspicious transactions. Thus, it was necessary to read internal documents on this topic to understand what constituted an unusual transaction from the perspective of the financial institution.

Given the reporting requirements—that individuals must make a report where they have reasonable grounds to suspect the transaction is related to money laundering or terrorist financing—tellers were a key demographic to include in this study, as they are primarily responsible for conducting transactions in branch that could be reported. Supervisors and managers were also included for participation as tellers might refer to them for authorization on transactions that were beyond their initialling limit[4] and which, in that case, might prompt a supervisor to advise an employee to file a UTR. Further, as supervisors and managers are responsible for ensuring that employee training is current and documenting employee awareness of their legal obligations (Manual), it is important to understand how they might direct their employees to submit reports of suspicion. In all, 19 tellers, 11 customer service managers, and 10 employees with mixed cash and supervisory responsibilities participated in this research.

This research relied upon semi-structured interviews, specifically using vignettes to prompt participants into describing how they might react to a particular client request.

4 Initialling limits are dollar limits placed on employees' autonomy. They are boundaries within which an individual can independently process transactions without secondary authorization. New employee limits may be very low—a few hundred dollars—whereas more senior employees may be able to process thousands of dollars worth of transactions independently (Iafolla, 2004), and initialling limits represent the degree of trust (or risk tolerance) the bank has for employees to act independently.

As client confidentiality and privacy, as well as s.8[5] of the *PCMLTFA* precluded observations of actual client-teller or client-manager interactions, this research used vignettes describing deposit, withdrawal, and wire transfer transactions to provide employees with a framework for describing their thoughts and actions in potentially unusual situations. Vignettes are particularly useful for systematically grounding "decision-making processes" (Daly, 1987, p. 268), as they provide an opportunity to "probe informants about the way they understand these scenarios and the potential solutions that are available to the people depicted in them. The answers that informants formulate with regard to these scenarios give insights into the values and attitudes that underlie their understandings" (Torres, 2009, p. 94). Where observation of real-life phenomena is not possible, vignettes provide an opportunity to understand how individuals react to a particular phenomenon.

The vignettes relied upon in this research posed scenarios of typical transactions. They asked employees to describe how they would act if presented with client transaction requests that might constitute unusual transactions according to banking best practices. The vignettes were meant to prompt employees to discuss their perspectives on conducting transactions for clients that might be unusual. For example, bank employees were asked to describe how they might proceed if a client presented different amounts of money for deposit, or requested to wire funds overseas. These vignettes were used as a means of inquiry into the ways employees who are not normally responsible for crime detection or investigation in the course of their employment discharge that duty: employees were asked about how they might handle a situa-

5 While the goal of this research was most certainly not to impede a current or future criminal investigation, s.8 of the PMLTFA stipulates that "[n]o person or entity shall disclose that they have made a report under section 7, or disclose the contents of such a report, with the intent to prejudice a criminal investigation, whether or not a criminal investigation has begun." The bank was concerned that observing client interactions from behind the teller wicket might somehow alert money launderers or financiers of terrorism that a report of suspicion might be submitted about their particular financial transaction.

tion that required a mandatory policing response in the form of a UTR. There are real concerns regarding the offloading policing functions, particularly to individuals who are not normally tasked with investigative functions (Favarrel-Garrigues, Godefroy & Lascoumbes, 2009). It is important to understand how these individuals interpret their roles as 'detectors of money laundering and terrorism financing', how they actually perform the work required of them by the law, and what the implications of that work might be for the clients who use in-branch banking services. Why do employees believe they must file reports of suspicion, and what might the unintended consequences (Ayling & Grabosky, 2006) of filing such reports be?

Employee Experiences of Policing Unusual Transactions

This section provides an account of some of the motivating factors that underlie the UTR. As retail branch employees use discretion to fulfil their government-mandated policing obligations, it is important to understand how they wield that discretion. Bank employees are required to actively police the transactions they process daily. This section therefore sheds light on how employees understand their mandate to identify suspicious transactions and why employees decide that a transaction should be reported, providing some insight into some of the factors employees take into account when they decide a transaction merits a UTR.

Why File An Unusual Transaction Report?

Perhaps unsurprisingly, employees largely cited legal and regulatory obligations as key reasons for which they would submit an Unusual Transaction Report. Legal and regulatory obligations were a key motivation for all employees:

> The government makes us do it. We have to do it so we can catch money launderers (Teller H1).
>
> This is how they [the government] catch criminals (Teller C2).

> Well, we do it because… It's the law, you know. And it's a part of my job, but it's something that we do because the law says we have to. All those anti-money laundering and anti-terrorism laws, that's why we have to do it (Manager B).

> They changed the requirements a few years ago. […] We have to report unusual transactions, money laundering or terrorist financing. It's the law, it used to be just money laundering but now we have to report terrorism, too. We have to do UTRs, so if they [the tellers] think it's unusual I will tell them to do it. They have to do it; it shows them [the regulators] that we are in compliance, and that [ensuring compliance] is a part of my job (Manager C).

For all 40 participants, legal and employment obligations were cited as reasons to submit a UTR. These responses were typical of reasons employees gave for submitting reports: policing money laundering or terrorist financing, for many, was not necessarily a 'natural' part of their jobs—which, otherwise, were focused on customer service—but an additional function imposed upon them by external legislative forces. While bank tellers—like Shearing and Stenning's archetypal Disney employees (1983)—have security functions embedded in their duties as employees, the imposition of a public policing function onto individuals working at private, for-profit companies suggests a blurring of policing roles consistent with what Mazerole and Ransley (2005) describe as "third party policing," where third parties are charged with a public policing function. Each bank employee cited legal reasons for submitting reports of suspicion, describing it as something that was external to, and perhaps not an integral part of, working in financial services. Unlike preventing frauds from being perpetrated against the bank, which is a routine part of the job (Iafolla, 2004), employees described detecting unusual transactions as a legal or regulatory obligation. In this way, the task of identifying and documenting transactions that may be related to money laundering or ter-

rorism financing is understood to be external to other security functions they might provide that are consistent with the profit-building goals of the bank.

That employees understand money laundering and terrorism financing detection to be external to their jobs—which are in fact focused around customer service and profit-building on behalf of the institution (Manual)—is also supported by their descriptions of the negative outcomes they might face for failing to report a transaction that is eventually revealed to be part of a scheme to finance terrorism or launder money. More than half of the employees who participated in this study cited penalties as a key motivator for them to submit unusual transaction reports. 26 of 40 participants—slightly more than half—spoke at length about their individual risk of being fined or jailed for not flagging a suspicious transaction:

> Teller: If we don't help them [FIU[6]] by reporting them, and they don't catch them, then the bank can get in trouble.
>
> Interviewer: What kinds of penalties are there?
>
> Teller: Well, fines. I think they can be big. Thousands and thousands. […] I don't know if it ever happened, but I don't want to be the first one. And if I was the first one—can you imagine? I would be fired, for sure. (Teller G2).
>
> Teller: The fines are huge. [laughs] I think they're bigger than what I make in a year, really, just, like, huge fines.
>
> Interviewer: Is it only you who gets fined, or is it the bank that gets fined, or…?
>
> Teller: Oh, gosh, it's both, I think. And it's really bad, too—if we don't report a transaction and it's terrorism or whatever, or if you tell someone that you're reporting it—it's called tipping—I think—I think you can go to jail. They're really serious, the government, it's really serious. It's not like you lose your [bonus] or something

6 The FIU is the bank's Financial Intelligence Unit which analyzes UTR and other reports before submitting them to Fintrac.

[laughs]. I'm not here to get fined, right? And I'm not going to jail. So I just do it. [laughs] (Teller B2).

Interviewer: Can you tell me if there's ever been a time where you weren't sure if you should report a transaction, and you didn't?

Teller: [thinks] No, no. If I think it's unusual, I submit it.

Interviewer: What if you're not sure? Like, if it might be unusual, or it might not be unusual…. What do you do in a case like that?

Teller: Well, even if I'm not sure, I would submit a UTR. […] If I do and there's nothing wrong, nothing happens, it's no problem. But if I don't, then I could get fined, or the bank could get fined. They [the government] are strict about it, and it's not good to get fined, and you know, it's expensive—they can fine you and the bank too, so it's a big deal. I would submit it, anyways. Nothing bad will happen if it's okay, so I just go and file the UTR (Teller I1).

Interviewer: You mentioned that you could be fined if you didn't submit a UTR. Do you know if that has ever happened to anyone at this bank?

Teller: No… [pause] No, I don't know, no. But our training that we do, it tells us that we can get fined for not doing a UTR.

Interviewer: Do you know how much the fine is?

Teller: I don't know for sure, but it is really a lot of money.

Interviewer: Do you have a rough idea? A thousand dollars, a hundred thousand dollars, a million dollars…?

Teller: Maybe a hundred grand? I don't know for sure, like I said, but it's a lot. And you can go to jail, too.

Interviewer: Really? For not submitting a UTR?

Teller: I think, yes. And for telling the customer that

> you did a UTR. So, I would just do it, because if I don't it could be very bad (Teller K1).

As Mazerolle and Ransley (2006) describe, third-party policing is undertaken non-state actors who "carry the burden for initiating some type of action that is expected to alter the conditions that that allow crime activity to grow or exist" (2006, p. 198). This burden is usually derived from a legal authority that delineates the parameters of third-party policing activity, including "the limits of their legal ability to cooperate with, or be coerced by, the police" (Mazerolle & Ransley, 2006: 199). While, arguably, "the police" do not figure in the considerations of employees—indeed, not a single participant made mention of the police in this regard—the coercive power of the law, with its penalties and prison sentences, presented concerns for almost two-thirds of participants. If the law's coercive power is so salient for employees, reports may be driven not by careful evaluation of the 'industry best practices' but by a kind of precautionary logic focused on mitigating not the risks to society that the law is focused on, but individual risks that employees perceive would have severe personal consequences[7].

Unusual Transactions and Suspicious Characters

When making the decision to submit reports of unusual transactions, the law requires that individuals ground their decisions based on "what is reasonable in your circumstances, including normal business practices and systems within your industry" (Fintrac, 2010a). While this is presented within the financial institution as part of its best practices (Bank Manual), employees described very different motivating factors for submitting reports of suspicion. Though the reports themselves are titled 'Unusual Transaction Reports' and 'Suspicious Transaction Reports,' employees often cited "weird," "funny," or "strange" behaviour as motivation to submit a UTR. Of the 40 employees interviewed, 27 presented 'atypical' behaviour or demeanour—that which was weird,

7 Many thanks to my reviewers for their imput on this point.

funny or strange—as the impetus for submitting an Unusual Transaction Report.

> They [FIU] need us to tell them if our customers are acting weird. They can't see them [the clients], so if we don't tell them, how are they going to know? (Teller D3).
>
> And a red flag for me is if he comes in with sunglasses on a really dreary day. There's no need for that. Why? On a really dreary day? Why don't you take your glasses off? You don't want me to see your face? You're hiding your face from me? You're inside! (Manager D)
>
> They're in front of us [laughs]. We can see them, like, if they're being strange, or if something is strange about what they're doing. Like if they are antsy, if they're making you hurry. What's the problem? Why don't you want to answer my questions? So if they act strange, then, yeah, I'd submit a report (Teller F1).
>
> Manager: If the customer seemed as if he was—if I got a funny feeling from him, because normally your instincts are correct, but if I got a funny feeling from him, I'd fill one out.
>
> Interviewer: What does it mean; he gives you a funny feeling?
>
> Manager: Um…. Well, customers that are—that have never been in the branch, or are talking to you, also, maybe they're overly friendly. A lot of the times people talking to you about nonsense are trying to distract you in some way. Or if a customer is hesitant in giving us ID, or is nervous in answering questions. That gives me a funny feeling (Manager K).

In contrast to the largely automated, computer-driven systems of intelligence gathering, employees in retail branches cited appearance and behaviour as a particular form of intelligence that they could offer in their UTRs. Client behaviour was a common reason to submit a report, especially because individuals in the FIU would have no

way to access that information otherwise. Branch-based UTRs offered the opportunity for employees to draw attention to clients behaving 'unusually,' although what was unusual varied widely, from wearing sunglasses in the branch to being 'too friendly'.

This focus on behaviour is accepted at the branch level as an important reason for submitting reports: indeed, how client behaviour 'made employees feel' was an important reason for submitting a UTR, and a wide variety of behaviours were cited. In its Guideline 2, Fintrac does cite behaviour as one of many reasons for which a transaction might be reported, pointing to the kinds of behaviours[8] that should be the focus of flagging a transaction:

> An assessment of suspicion should be based on a reasonable evaluation of relevant factors, including the knowledge of the customer's business, financial history, background and behaviour. Remember that behaviour is suspicious, not people. Also, it could be the consideration of many factors—not just one factor—that will lead you to a conclusion that there are reasonable grounds to suspect that a transaction is related to the commission or attempted commission of a money laundering offence, a terrorist activity financing offence, or both. All circumstances surrounding a transaction should be reviewed (2010b: 15-16).

In this light, the importance placed upon client behaviour when deciding to submit a UTR *may* be reasonable when viewed within a totality of circumstances. What employee responses demonstrate, however, is that employees may not give as much consideration to the *financial* behaviour of a client as they do to the personal characteristics, actions and activities of clients in the branch. Bank employees are trained

8 This description is made with reference to Suspicious Transaction Reports; as described above, STRs are only submitted by banks after UTR reports have been investigated and corroborated. Still, STR guidance informs the training programs that employees must take and pass annually, and to that end, employees must follow STR guidelines when submitting UTRs.

to identify and to interpret risky patterns of financial activity (Iafolla, 2004) much more rigorously than they are to analyze the friendliness or surliness of their clients.

In many cases, it may be much easier to impartially interpret patterns of financial behaviour than to imbue meaning into the 'friendliness' of clients, particularly if employees focus on a client's attitude or conduct is the sole or main reason for submitting a UTR. Still, Fintrac's (2011) Guidance on this issue specifies that suspicious behaviour, and not suspicious people are of concern. If the behaviour described by employees is not grounded in other industry-identified 'red flags'—those normative boundaries that the PCMLTFA cites as reasons to report financial transactions—UTR reporting may in fact capture subjective suspicion of individuals, and not necessarily suspicion of an unusual transaction. Interpreting the 'totality of circumstances' with regard to suspicious transactions may indeed include assessments of client behaviour; still, those assessments are subjective and—unlike recorded financial transactions—cannot be reinterpreted by subsequent parties. The only record of the 'suspicious behaviour' is the employee's individual impression. Where those impressions direct the reporting process, the investigative net may widen to (unfairly) capture transactions that are in no way suspicious but for the fact that the client is behaving in a way that may not be socially normative, but otherwise unsuspicious.

Discussion

Although intended to be grounded in industry best practices, suspicion-based transaction reporting may instead be grounded in individual perceptions of client behaviour, or motivated by self-interest. UTRs are generated by individual employees' perceptions of the legitimacy of client transactions instead of thoughtful accounts of suspicious financial behaviour, and, in many cases, motivated by concerns for one's own security. The possibility of time spent incarcerated or hefty fines to be paid were at the forefront of employee

decisions to file UTRs. This raises questions regarding both the efficacy and justness of this process.

Certainly, third-party policing in this area has laudable policy objectives: preventing the abuse of Canada's financial systems by money launderers or financiers of terrorism is an important policy objective, and one which may best be accomplished by making the reporting of financial transactions by financial institutions mandatory. Mandatory reporting obviates problems with getting financial institutions to comply with reporting requests by transforming them into reporting requirements (Ayling & Grabosky, 2006), and certainly, cash transaction reporting requirements are a common element of financial regulation in advanced capitalism (Reuter & Truman, 2004). But what are the possible unintended consequences of mandating front-line bank employees to engage in policing on behalf of the state?

Levi notes that downloading suspicious transaction reporting to financial institutions "offers the possibility of policing in a less prejudiced way than by use of police discretion" (2002, p. 189), particularly because the banking industry relies in part on data mining and computer analytics methodologies (Zdanowicz, 2004) that focus on patterns of financial activity. Analytics strategies are understood to be 'less prejudiced' precisely because of their focus on patterns of financial behaviour and not on interpersonal cues that may be misread or misinterpreted. Financial institutions certainly do rely upon analytics for identifying unusual transactions: indeed, it is expected that financial institutions devote staff to investigating the intelligence gleaned from computer systems. Regardless, where front-line staff are concerned, it appears that downloading the policing of money laundering and responsibilizing bank personnel, thereby requiring them to undertake a policing function, has in many ways simply replaced the suspicion-based investigating (Levi, 2002) of the police.

At first blush, downloading suspicion-based reporting to industry makes sense. Patterns of behaviour can be revealing, identifying activity that is consistent with the suspicious

behaviour that is targeted by the PCMLTFA. For example, smurfing—the practice of structuring transactions in smaller amounts in order to circumvent currency threshold reporting requirements (Fintrac, 2010a)—is defined by financial activity. If patterns of activity are the focus, bank employees are well-positioned to identify and report those transactions. However, suspicion-based reporting becomes murky when demeanour is the focus of reports. A UTR filed on the basis of subjective interpretations of behaviour may not accurately capture a transaction that is in fact money laundering or terrorism financing. Bank employees, in the course of conducting such transactions, may inquire into the source of funds (Fintrac, 2011a), and in the course of their inquiries may take note of client behaviour (Bank Manual). If behaviour is the sole focus of a UTR, any number of ideas about how a client 'ought' behave become justification for a report of suspicion. For example, a preference for leaving on one's sunglasses—explainable for any number of reasons—may be just as suspicious as a deposit of several thousand dollars with no supporting documentation or reasonable explanation.

This is particularly important to consider in the context of a permissive reporting regime. Individuals are required to report suspicious transactions, and the letter of the law is not black-and-white in this area. Beyond threshold transaction reports, where a particular dollar amount prompts the reporting process, there is very little in terms of specific detail regarding what actually is suspicious. According to s.10 of the PCMLTFA, there are no legal penalties for submitting a Suspicious Transaction Report in good faith that turns out to be unfounded. When suspicion hinges on the smallest fragment of atypical behaviour, the net of surveillance may widen to include individuals whose transactions are not suspicious. Bank employees should not fear adverse consequences for submitting reports of suspicion in good faith, but it is problematic that individuals opted to submit a transaction because 'nothing bad' will happen to a customer

if their suspicions are incorrect. While a criminal charge may not result or assets may not be seized if a transaction is legitimate, submitting UTRs out of a concern for one's own safety, or because a client's behaviour is 'unusual', raises important considerations about justice. A lack of adverse outcomes for the client, or the client's ignorance of increased scrutiny, does not justify widening the net of surveillance.

Finally, and perhaps most crucially in the post-9/11 context, is how subjective reporting may impact the financial lives of religious, ethnic, or racial minorities. Suspicion-based reporting should not be influenced by assumptions regarding race, ethnicity, and illicit financial transactions. Reports of suspicious transactions motivated by self-concern or based on idiosyncratic concerns regarding customer demeanour are in themselves troubling, but other responses from participants in this study suggested that race, religion, and ethnicity may inform the submission of UTRs. Under the law, these demographic characteristics are not meant to inform the reporting process; however, there may be slippage in the minds of bank employees between "what is suspicious" and "who is suspicious". Although beyond the scope of this paper, preliminary results from this research do suggest that front-line employees are concerned about the impacts of suspicion-based reporting on minority groups, particularly in a culture where precautionary logic motivates the reporting process. The entrenchment of what O'Malley (1992) would refer to as 'prudentialism' in a suspicion-based reporting regime carries the potential for extralegal factors to creep into the policing process, as third-party police are encouraged in this context to make reports based on their subjective suspicions.

Conclusion

When the 2001 amendments to Canada's proceeds of crime legislation were passed, suspicion-based transaction reporting had not yet become pervasive: according to Fintrac (2011b), approximately 100 discrete reporting entities submit-

ted at least one STR, but by the end of the decade that number had increased to more than 900 discrete entities. While this research has focused on the Unusual Transaction Report, which may not crystallize into a firm report of suspicion in the form of a Suspicious Transaction Report, the trends in reporting and the broader reporting landscape point to an important consideration: the surveillance apparatus in the banking industry is sufficiently developed to necessitate the UTR. In the absence of this apparatus—a unit of investigators devoted to examining each report of unusual activity—reports are sent directly to Fintrac in the form of Suspicious Transaction Reports.

The entrenchment of third-party policing in financial institutions is troubling. Financial institutions act as entry points and facilitators for economic participation, and the overwhelming majority of Canadians rely on banks to ensure they can perform important yet routine financial transactions. Legally mandating private citizens working in the private sector to engage in a policing function on behalf of the state is troubling not only because it extends the policing powers of the state into the private sector, but also because it does so in ways that diminish accountability and transparency[9]. Financial services are embedded in social relations, and developments in third-party policing such as mandatory suspicious transaction reporting present an opportunity for the state to harness corporate power for ends that may have important implications for the ways in which citizens experience state power in general and policing in particular.

The intersection and concentration of corporate and state power in financial services is more than just the making of strange bedfellows. By moving the policing of this activity just beyond the state, the traditional mechanisms for holding the public police accountable no longer apply. How clients who suffer adverse consequences to their ability to access financial services have recourse, and who should be held accountable—the bank, doing policing, or the government, requiring banks to engage in policing—is unclear.

9 Many thanks to my reviewers for their insights on this point.

Harnessing the power of private entities for use by the state is problematic. When policing activities are downloaded beyond the control of the state, and where sanctions provide motivation for engaging in policing activities, the nature of policing itself is transformed. Accountability and transparency may come at the cost of increasing the power of the state and reach of the state into private sector activities. Financial services is no exception, and the potential reach of the state through this sector is vast, and the implications for security and justice are serious.

References

Ayling, J. and P. Grabosky. (2006). Policing By Command: Enhancing Law Enforcement Capacity Through Coercion. *Law and Policy,* 28(4), 420-443.

Beare, M. E. and S. Schneider. (2007). *Money Laundering in Canada: Chasing Dirty and Dangerous Dollars*. University of Toronto Press: Toronto, ON.

Brodeur, J.P. (2010). *The Policing Web*. Oxford University Press: New York.

Brown, J. and R. Lippert. (2007). Private Security's Purchase: Imaginings of a Security Patrol in a Canadian Residential Neighbourhood, 49(5): 587-616.

Canadian Bankers Association. (2012). *How Canadians Bank*. Retrieved August 24, 2012, from Canadian Bankers Association web site: http://www.cba.ca/en/media-room/50-backgrounders-on-banking-issues/125-technology-and-banking.

Canadian Peace Alliance. (2001). Open Letter to Prime Minster Jean Chrétien Opposing Bill C-36. Retrieved November 27, 2012, from Canadian Peace Alliance web site: http://www.acp-cpa.ca/C-36openletter.htm.

Daly, K. (1987). Structure and Practice of Familial-Based Justice in a Family Court, *Law and Society Review,* 21(2), 267-290.

Daniels, R.J. (2001). Introduction in R. J. Daniels, P. Macklem, & K. Roach (Eds.), *The_ Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. University of Toronto Press: Toronto, Canada.

Daniels, R.J., P. Macklem, & K. Roach (Eds.). (2001), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. University of Toronto Press: Toronto, Canada.

Davis, K.E. (2001). Cutting off the Flow of Funds to Terrorists: Whose Funds? Which Funds? Who Decides? in R. J. Daniels, P. Macklem, & K. Roach (Eds.), The Security of *Freedom: Essays on Canada's Anti-Terrorism Bill*. University of Toronto Press: Toronto, Canada.

De Koker, L. (2009). Identifying and managing low money laundering risk: perspectives on FATF's risk-based guidance. *Journal of Financial Crime*, 16(4), 334-352.

Duff, D.G. (2001). Charitable Status and Terrorist Financing: Rethinking the Proposed *Charities Registration (Security Information)* Act in R. J. Daniels, P. Macklem, & K. Roach (Eds.), The Security of *Freedom: Essays on Canada's Anti-Terrorism Bill*. University of Toronto Press: Toronto, Canada.

Favarel-Garrigues, G., T. Godefroy, & P. Lascoumes. (2008). Sentinels in the Banking Industry: Private Actors and the Fight against Money Laundering in France. *British Journal of Criminology*, 48(1), 1 - 19.

Financial Transactions and Analysis Centre of Canada. (2010). *Fintrac Annual Report 2010: Ten Years of Connecting the Money to the Crime.* Retrieved August 24, 2012, from Fintrac Web site: http://www.fintraccanafe.gc.ca/publications/ar/2010/ar2010-eng.pdf

Financial Transactions and Analysis Centre of Canada. (2011). *What Must Be Reported?* Retrieved August 24, 2012, from Fintrac Web site: http://www.fintrac.gc.ca/publications/brochure/05-2003/2-eng.asp.

Financial Transactions and Analysis Centre of Canada. (2012a). *Reporting to Fintrac.* Retrieved August 24, 2012, from Fintrac Web site: http://www.fintrac.gc.ca/reporting-declaration/1-eng.asp.

Financial Transactions and Analysis Centre of Canada. (2012b). Who Must Report? Retrieved August 24, 2012, from Fintrac Web site: http://www.fintrac.gc.ca/reporting-declaration/Info/re-ed-eng.asp.

Johnston, L. (2000). *Policing Britain: Risk, Security, and Governance*. Harlow: Pearson Education (Longman Criminology Series): Essex, UK.

Iafolla, V. (2004). A Risky Business: The Governance of Security in Retail Banking. *Oral presentation at the Canadian Society of Criminology Conference*. Toronto, ON.

Iafolla, V. (2011). June. National Security, Civil Liberties and Identity: the 2001 Antiterrorism Debates in Canada. *Oral presentation at the Canadian Sociological Association Meetings*. Fredericton, NB.

Levi, M. (2002). Money Laundering and its Regulation. *The ANNALS of the American Academy of Political and Social Science*, 582, 181-194.

Mazerolle, L., & Ransley, J. (2006). The Case for Third-Party Policing. In D. Weisburd & A. Braga (Eds.), *Policing Innovation: Contrasting Perspectives* (pp. 191-206). New York: Cambridge University Press.

Murphy, D.P. (2003). Canada's Laws on Money Laundering and Proceeds of Crime: The International Context. *Journal of Money Laundering Control*, 7 (1), 50.

O'Malley, P. (1992). Risk, power and crime prevention, *Economy and Society*, 21(3), 252-75.

Osborne, D. and T. Gaebler (1992). *Reinventing Government*. Addison-Wesley Publishing Co.: Reading, Mass.

Proceeds of Crime (Money Laundering) and Terrorist Financing Act. (S.C. 2000, c.17). *Revised Statutes of Canada*. Retrieved August 24, 2012, from the Department of Justice Canada Web site: http://laws-lois.justice.gc.ca/eng/acts/P-24.501/.

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

Rigakos, G. and D. Greener. (2000). Bubbles of Governance: Private Policing and the Law in Canada, *Canadian Journal of Law and Society* 15(1): 145-185.

Roach, K. (2001). The New Terrorism Offenses and the Criminal Law in R. J. Daniels, P. Macklem, & K. Roach (Eds.), *The Security of Freedom: Essays on Canada's Anti-Terrorism Bill*. University of Toronto Press: Toronto, Canada.

Roach, K. (2003). *September 11: Consequences for Canada*. McGill-Queens University Press: Quebec City, PQ.

Shearing, C., and Stenning, P. (1983). Private Security: Implications for Social Control, *Social Problems* 30(5): 493-506.

Shearing, C., and Stenning, P. (1984). From the Panopticon to Disney World: The Development of Discipline in A.N. Doob and E.L. Greenspan (Eds.), *Perspectives in Criminal Law*. Canada Law Book: Aurora, ON.

Shearing, C., & Wood, J. (2003). Nodal Governance, Democracy, and the New 'Denizens', *Journal of Law and Society*, 30(3), 400–19.

Torres, S. (2009). Vignette Methodology and Culture-Relevance: Lessons Learned through a Project on Successful Aging with Iranian Immigrants to Sweden. *Journal of Cross Cultural Gerontology*, 24(1), 93-114.

Verhage, A. (2009). Supply and demand: anti-money laundering by the compliance industry, *Journal of Money Laundering Control*, 12(4), 371 – 391.

Zdanowicz, J. S. (2004). Detecting money laundering and terrorist financing via datamining. *Communications of the ACM – New Architectures for Financial Services*, 47 (5), 53-55.