Law and surveillance invariably go hand-in-hand. Indeed, there are few occasions where one is present without the other, particularly as notions of law and legality are expanded to encompass not only ‘rules’ but also ‘norms’ (Rose and Valverde 1998). While this assertion is unlikely to be controversial, the examination of the relationship between law and surveillance has been quite limited in the ‘Surveillance Studies’ literature. More often than not, law is viewed either as part of the enabling framework of surveillance, providing legal authorization for specific surveillance measures or, as is more often the case, a means of reasserting control and limiting the scale or scope of surveillance. For example, in the otherwise excellent Routledge Handbook of Surveillance Studies, law explicitly appears only in the final section and then only as a means of “limiting surveillance” (Ball, Haggerty, and Lyon 2012). This limited treatment of law as either a form of authority or source of restraint is accompanied by the prevailing assumption that there is “too much surveillance” and that we are all members of a “surveillance society.” Within this framework, surveillance is viewed as a form of power that proceeds through a logic of visibility conceived first through the metaphor of the camera and the visible body and later through the surveillance of digital identities and online lives. This dynamic of visibility and associated forms of social sorting is, after all, why too much surveillance is deemed troublesome and inherently so.

While applicable to many contexts in which contemporary forms of surveillance are operative, these analytical tendencies become more problematic as we follow surveillance into other domains, none more so than the world of financial markets where it is the absence rather than the prevalence of surveillance that is the problem and where law often figures as a source of restraint embedded within, rather than external to, surveillance and regulatory systems. The first two questions meant to inform this debate—“can law be the answer to too much surveillance in an era of mass surveillance?,” and “can surveillance be the answer to too much law in an era of legalization of society?”—thus may not apply as the issue is neither “too much surveillance,” nor “too much law.” In fact, I would pose a slightly different question. In light of the efforts over the past ten to fifteen years to innovate and develop new forms of “financial surveillance” (Williams 2009, 2013) geared towards the identification of financial and market misconduct, the question is whether surveillance may be the answer to the absence of law or, more accurately, the failures of legal regulation. Given that law itself figures as a key factor in limiting the success of these new systems, examining financial surveillance provides a very different way of thinking not only about surveillance but also the relationships between surveillance and law. The remainder of this essay explores these very dynamics starting with the notion that financial surveillance is on the rise and is an increasingly important strategy in combating financial and market misconduct.
While dwarfed by the expansion of surveillance in other fields, including CCTV, drone technologies, and online surveillance and data mining, surveillance has also taken off in the financial sphere expanding dramatically in scope and intensity over the last ten years. Rather than the surveillance of markets by corporations and financial institutions with the objective of gaining market intelligence and thus furthering their profit-making activities, here I am referring specifically to the surveillance of these very financial actors by regulatory authorities. Thus, the term ‘financial surveillance’ as it is used here refers to the technologies, logics, and practices associated with monitoring the financial sphere for legal and/or regulatory purposes (Williams 2009, 2012, 2013). In tracing the rise of financial surveillance, two developments are especially noteworthy.

The first is the real-time surveillance of financial markets. Starting in the 1990s, self-regulatory organizations (SROs) in Canada, the United States, and several other jurisdictions began to develop software applications that could systematically monitor market transactions for signs of insider trading, market manipulation, and a host of other regulatory concerns. These applications were rooted in, and driven by, technological changes within the markets themselves as the face-to-face transactions conducted in open trading pits were eclipsed by fully automated and electronic exchanges (Zaloom 2006). With the resulting increases in the speed and volume of transactions putting the markets beyond the reach of human oversight, steps were taken to develop computer-mediated and automated surveillance systems. The 2008 financial crisis has served to further bolster these investments with agencies such as the Financial Industry Regulatory Authority (FINRA), the industry-funded SRO responsible for overseeing U.S. stock markets, recently announcing an expansion of its surveillance programs to include more effective cross-market surveillance as well as greater oversight of so-called ‘dark-pool’ trading (Bunge and Patterson 2013).

Another key development is the greater use of fraud detection software to uncover anomalies in financial statements and thus potential indications of accounting abuses. This is epitomized by the U.S. Securities and Exchange Commission’s new “Accounting Quality Model” that seeks to use quantitative analytics to identify anomalies in the financial statements of publicly traded companies (Eaglesham 2013). The agency has also developed new software that analyzes word choices in corporate annual reports for signs of earnings manipulation (Eaglesham 2013). Other applications abound, including software that trolls websites and online discussion boards for signs of market manipulation and insider trading. It is thus not an overstatement to say that financial surveillance has emerged as a serious and significant activity that promises greater oversight of financial actors and markets. And yet, the question invariably emerges: how successful or useful are these surveillance tools and technologies in practice? Do they really matter and can they deliver on their promise of enhancing market oversight? It is here that law and questions of legality become significant in a way that departs from their treatment in the Surveillance Studies literature.

Drawing from my research on financial surveillance in Canada (Williams 2009, 2012, 2013), one of the key ways in which law has constrained the surveillance efforts of financial regulators and thus impacted their effectiveness involves the question of jurisdiction. While typically conceived in terms of the boundaries between state territories, jurisdiction viewed more broadly as the legal encoding of space and enactment of legally bounded territories (Blomley and Bakan 1992; Blomley 1994; Ford 1999; Lange 2003) exerts two critical effects on the scope and scale of financial surveillance. First, regulators are typically limited to individual markets or exchanges and are thus prevented from engaging in cross-market surveillance, a significant constraint given that manipulative activity often occurs across different markets. While markets have themselves become increasingly interconnected and networked, regulatory surveillance systems remain largely confined to individual silos with each individual regulator only able to see a small slice of market activity. There is also the problem that many exchange platforms and trading venues are exempted from regulatory oversight and are thus entirely removed from surveillance systems. Prior to the 2008 financial crisis, these ‘private’ spaces of exchange spanned a vast domain including the over-the-counter derivatives market which was explicitly exempted from regulatory oversight as well as so-called ‘dark pools’ where large, primarily institutional investors traded under the cover of secrecy.
While post-crisis measures, many of which have been mandated by the U.S. Dodd-Frank Reform and Consumer Protection Act (2010), have exposed some of these activities, large swaths of trading activity remain largely invisible and thus escape and exceed surveillance and regulatory capabilities.

A second respect in which legal jurisdiction has served to constrain the impact of surveillance efforts involves the division of labour among regulatory agencies, namely the self-regulatory organizations that perform much of the surveillance activity and the statutory agencies typically responsible for responding to market troubles once revealed. A perfect example of the jurisdictional tensions between regulators comes from the Canadian context where the real-time surveillance of financial markets is the responsibility of a self-regulatory organization, the Investment Industry Regulatory Organization of Canada (IIROC). However, in the event that irregularities are discovered that may be indicative of insider trading (e.g. high levels of trading in a given stock leading up to the public announcement of a takeover or major acquisition), the agency is required by statute to turn the case over to the appropriate provincial securities regulator. This has emerged as a major source of tension as the SRO works to uncover what it believes are significant and impactful cases only to pass them to the securities commissions where they often disappear, never to be heard from again (Williams 2009). It is thus not only the areas of invisibility produced by the carving up of regulatory territories, but also the emergence of inter-agency conflicts and attendant regulatory politics that undermine the impact and meaningfulness of surveillance efforts.

Beyond jurisdiction and the configuration of regulatory networks relative to the markets, another key respect in which law serves as a barrier to market surveillance involves access to market data. Here we move from real-time monitoring of the markets to a very different form of ‘financial surveillance’ rooted in the ability of outside researchers to access trading data and conduct their own analyses focusing on market problems that may exceed the capabilities or interests of regulators themselves. The difficulty, and the point where law once again intervenes, is that these data are deemed by the industry to be proprietary and thus confidential. An example of how this legal claim has served to limit market transparency and the potential benefits of more fulsome disclosure of trading involves the Commodity Futures Trading Commission (CFTC) which is responsible for overseeing U.S. commodities and derivatives markets. By law, financial exchanges are required to provide daily trading data to the CFTC for regulatory and compliance purposes, a requirement that has expanded in the wake of Dodd-Frank to include swaps and other instruments traded in the over-the-counter market. In several cases, the CFTC has made these data available to qualified outside researchers under its access program for visiting academics. Drawing from these data, a handful of studies emerged that were critical of high-speed trading with one report linking this form of trading to the 2010 “flash crash,” and another identifying harmful effects on small investors (Lynch 2013). In response, legal counsel for the CME Group Inc., the world’s largest futures exchange, sent a letter to the CFTC reminding them these data were proprietary and their use “for the preparation of non-Commission sponsored publications” violated federal law protecting trade secrets (Lynch 2013). Shortly thereafter the agency suspended the program, a clear signal of the legal limits of market transparency and ‘financial surveillance.’

What emerges from this brief foray into the world of financial markets is that when considering the nature of surveillance and in particular the relationships between surveillance and law, context really does matter. While it may often be the case that surveillance is rooted in a logic or “field of visibility” (Hier and Greenberg 2009; see also Haggerty and Ericson 2006) and that it is enabled rather than constrained by law, this does not necessarily hold in all contexts and circumstances. There are instances where law actively impedes surveillance, not as an external constraint but rather part of the internal limits of surveillance systems themselves, and where surveillance practices may render the world less rather than more visible. The financial sector is a case in point (see also Snider and Molnar 2013). Moving forward, more research is needed on these unique contexts and, in particular, the distinct challenges underlying the surveillance of rather than by corporate and financial actors. Within these contexts, we need to continue to
ask whether surveillance may be the answer to the absence of law, and whether the answer to this question lies within the nature and mobilization of law itself.

References