OFFICE OF THE
INFORMATION & PRIVACY
COMMISSIONER
— for —
British Columbia

LOCAL GOVERNMENTS AND THE GROWTH OF SURVEILLANCE

August 30, 2006

1.0 INTRODUCTION

British Columbia's municipalities have for decades had second-hand dealer and pawnbroker bylaws requiring reporting of information to police—the City of Victoria, for example, passed a second-hand dealers bylaw in 1916. In recent years, however, it has become more and more common for British Columbia's local governments to enact bylaws requiring businesses to collect their customers' personal information and provide it to local police agencies or licensing inspectors. We have seen in recent years an expansion of the types of businesses that are required to collect customers' personal information, the purposes for such requirements and the types of personal information which must be collected and handed over to police. New information technologies that enable quick and efficient distribution of personal information to police agencies, and its storage, have added a significant dimension to the trend.

For reasons expressed below, this Office strongly believes that municipalities should not be in the business of passing surveillance bylaws. They clearly have privacy implications of varying degrees, depending on the nature of the personal information being collected, for ordinary members of the public who are going about their lawful business. Among other things, the bylaws we reviewed contain no measures to ensure that personal information is used properly and is protected against unauthorized use or disclosure. Against the clear privacy impact of such bylaws, it is doubtful that such bylaws are really effective, and there are certainly tools that may more effectively achieve the community safety objectives that the bylaws purport to address. This Office is therefore firmly of the view that municipalities should not pass bylaws compelling citizens to give up their privacy in a wholesale and indiscriminate manner. Consistent with long-standing law and practice in Canada, it should be left to the courts to issue warrants or orders to businesses to turn over customer information on a case-by-case basis where justified.

2.0 DISCUSSION

2.1 Background

As bylaws forcing businesses to act as data collection agencies for government proliferated in kind and number, we became concerned that their privacy implications were not being considered.[1] For this reason, we asked a number of larger British Columbia municipalities and organizations to comment on the use of municipal bylaws to require businesses to collect personal information from their employees and customers and make the information available to municipal licensing staff and the police. We also obtained examples of bylaws, aimed at lawful businesses, requiring collection and disclosure to police of customers' personal information.

Most common are bylaws which regulate pawnbrokers, second-hand dealers and other vendors of used property (such as scrap metal merchants). These types of bylaws have a long history in municipalities. However, in more recent years, the concept of controlling other legal, but in the judgement of some, suspect activities through municipal bylaws has become more common. Municipalities have used the compulsory collection and reporting of personal information to control adult entertainment businesses such as escort services and body-rub parlours. Other activities which the police might find suspect such as private mailbox rentals,[2] sale of pepper spray[3] and the sale of hydroponic equipment[4] have increasingly become the focus of bylaws requiring collection of personal information.

The extent and kinds of personal information required vary. The most common requirement is for collection of name, address and description of the individual involved in the transaction. Having said this, many bylaws go further and require collection of more detailed descriptive elements such as height, weight, race, gender, eye colour, date of birth, picture identification and serial numbers from identification cards. In some cases, identifying information of a vehicle used to transport goods brought to a store is required.

Bylaws relating to pawnshops and second-hand dealers, for example, typically require business owners to record not only information identifying the item bought or pawned, but also details about the individual who transferred the item and even the person who bought the item. Bylaws usually require businesses to keep the personal information indefinitely and make it available for inspection by police and other authorities at any time. Bylaws often compel pawnshops to provide the police with daily records of their transactions in electronic form. The trend toward mandatory daily reporting of personal information and transaction details is on the increase, in part because of the availability of commercial software products to enable such reporting.

In the case of adult services such as escort agencies, businesses are typically required to record the identity of employees and customers and make this information available to licensing authorities and police. The City of Vancouver has such a bylaw. A City of Surrey bylaw regulating the sale of pepper spray requires the seller to document such things as the name, age, race, height and weight of anyone purchasing pepper spray and provide this personal information to police. At least one example can be found of a bylaw requiring businesses that rent out mailboxes to take customer details and turn these over to police.

Recent media reports indicate that the City of Richmond is considering a bylaw to require scrap metal dealers to record personal information of individuals who bring in scrap metal and provide this information to police. Early in 2006, the City of Chilliwack considered a bylaw that would require businesses selling fertilizer[5] or hydroponic equipment to record customer details and turn these over to police. Similarly, the City of Langley earlier this year considered a bylaw to require anyone selling drug paraphernalia to force customers to give up their personal information, and then hand that information over to police.

These are only a few examples of laws that essentially force private sector businesses to compile surveillance databases on their customers, *i.e.*, to keep registers of personal information of citizens for the primary purpose of monitoring legal behaviour. Some might argue that such databases only distinguish individuals engaged in legal-but-suspect activities from the general public, but they clearly have the potential to be invasive and discriminatory. They are undoubtedly a form of surveillance, under which the private sector is compelled to act as an agent of the state in collecting personal information and routinely turning it over to police.

Another trend has been to require businesses to electronically provide collected personal and other associated information to police. This has allowed police to obtain information almost immediately and check if property has been stolen or if the individuals involved are otherwise of interest to the police. In the latter case, the bylaws function, not to address stolen goods issues, but to facilitate the tracking and location of individuals wanted for whatever reason or—and this raises serious concerns—who are merely “of interest”. A further step has been the development of software which requires stores to enter all specified data, which is then forwarded directly to the police and which can then be uploaded to law enforcement information systems such as PRIME, British Columbia’s online Police Records & Information Management Environment. Nor do any of these bylaws that we examined address issues of further disclosure and use—for perhaps inconsistent purposes—of personal information in the databases they create.

2.2 Overview of responses to our request for comment

The responses we received from municipalities primarily consisted of bare assertions that local governments should be able to enact bylaws to regulate businesses which may be associated with criminal activity.

The most detailed responses to our request for comment came from the Union of British Columbia Municipalities ("UBCM"), the B.C. Pawnbrokers Association ("Pawnbrokers Association") and the B.C. Civil Liberties Association ("BCCLA"). The UBCM said that its executive, in reviewing the issue of such bylaws and our investigation, "wished to emphasize that the bylaws that your Office is reviewing have been adopted in the interest of protecting citizens and keeping them safe." The motives of municipal councils in passing such bylaws are not in question—we recognize that there are valid community concerns about marijuana grow-ops and other drug-related activities. The concern remains, however, that these bylaws are not a necessary or tailored response to the problem—they create other problems without offering any demonstrated law enforcement benefit in return.

The UBCM also provided a legal opinion on the question of whether the *Community Charter* confers authority on local governments to pass bylaws of the kinds described above. That legal opinion suggested that "inspection" under the authority of such bylaws is a means to permit local governments to ensure that businesses meet the appropriate standards set out in the bylaw. The collection of personal information is one of the means of inspection. As support, the opinion referred to the decision of the British Columbia Supreme Court in *International Escort Services v. Vancouver (City)*[6] and argued that s. 26 of FIPPA allows the collection of personal information for the purposes of law enforcement, with these surveillance databases being for law enforcement purposes.

There is no need to critique the UBCM opinion in any detail here. Suffice it to say that we have considered its analysis in depth and concluded that there are good reasons for concluding that the courts would, in fact, not share the generous view that the UBCM opinion expresses regarding municipal authority to pass personal information bylaws.

We acknowledge that, in recent years, Canadian courts have often deferred to local governments in deciding whether they have the authority to pass various types of bylaws, but empowering legislation such as the *Community Charter* does not confer limitless power on local government officials. There is real doubt about the validity of bylaws aimed at compelling businesses to collect and disclose customer personal information, where the bylaws contain no otherwise valid scheme for regulating businesses.[7] Indeed, *International Escort Services,* the court decision on which the UBCM opinion relies, held that municipalities are subject to significant limitations in passing bylaws to compel collection and disclosure of personal information.[8]

Elected municipal officials appear to share our doubt about whether the *Community Charter* authorizes municipalities to pass such bylaws—Lower Mainland politicians passed the following resolution at their meeting in May of this year:

> **R2 REGULATION OF HYDROPONIC AND DRUG PARAPHERNALIA BUSINESS**
>
> THEREFORE BE IT RESOLVED that the Lower Mainland Municipal Association and the Union of BC Municipalities request that the Province amend Section 59 of the *Community Charter* to give municipalities the clear authority to impose requirements on hydroponics and drug paraphernalia businesses, to the same extent they can impose requirements on second hand businesses.[9]

The BCCLA made three points. First, it argued that allowing police agencies access to these databases is essentially constructive search and seizure without judicial oversight. Section 8 of the *Canadian Charter of Rights and Freedoms* protects Canadians from unreasonable search and seizure without prior judicial authorization. The BCCLA maintained that police agencies are trying to use municipalities to obtain personal information without warrant, thus indirectly doing what the police could not do directly without violating the constitution.

Second, the BCCLA argued that such bylaws are outside the bylaw authority of local governments because they deal with criminal law, which only the federal government can legislate. The BCCLA maintained that the actual purpose of such bylaws is to monitor criminal activity—to legislate in respect of crime–-and that criminal law is outside the jurisdiction of local governments. The BCCLA cited a New Brunswick Provincial Court decision, *City of Fredericton and the Re-Purchase Shop*, in support of this position.[10] In that case, the Court held that a municipal bylaw requiring businesses to submit reports to the police was invalid because it was in the nature of a criminal law enactment, which only Parliament could enact.

Third, the BCCLA argued that such bylaws are discriminatory because they target the customers of these businesses for police monitoring. It argued that there "may be no discriminatory intent in these bylaws, but there is nevertheless discriminatory effect." Individuals who use the services of second-hand dealers or pawnbrokers often need to obtain money quickly and cannot use alternative methods of selling their possessions.

The Pawnbrokers Association said it does not object to bylaws that require pawnbrokers to keep registers of property they take in pawn and sell, but said it does not believe FIPPA allows local governments to force businesses to provide customer information to police agencies on a regular basis (as opposed to an item by item basis on inquiry by the police). It said that it recognizes the role of law enforcement in ensuring that property left with these businesses is not stolen. If property is stolen, it is a law enforcement matter and customer information for

the item identified as stolen can then be provided to police. The Pawnbrokers Association also argued that individuals who use these services to obtain small amounts of money have an arrangement between the customer and business which is similar to transactions between a bank and its customers and such a relationship should be subject to a reasonable level of confidentiality.

2.3 Why municipalities should not pass these bylaws

As indicated above, there is doubt as to whether British Columbia's local government legislation, the *Community Charter*, authorizes municipalities to enact bylaws that force businesses to collect and disclose to police personal information of business customers and clients, certainly outside the area of pawnbrokers and secondhand dealers. Regardless of whether such bylaws are legally valid—or constitutional under the *Canadian Charter of Rights and Freedoms*[11]—they raise serious privacy concerns in light of the proliferation of such initiatives and of other trends in law enforcement and information technology. The important policy question is whether, even if one assumes municipalities have the statutory authority to pass such bylaws, they should be passing them at all.

The scope and scale of databases containing personal information have grown exponentially in recent years, driven in part by developments in information technologies. There is good reason to suggest that governments in Canada and elsewhere are increasingly turning to computer technologies to compile and exploit personal information for ordinary law enforcement purposes, not just reasons of national security. There may be benefits from some of these initiatives, and privacy protections can be found to mitigate some of the privacy risks they raise, but concerns remain.

There is a danger that we will increasingly be judged by our digital personalities—the constructs of each of us that are created from the digital footprints we unwittingly leave each day. We commented on this danger in our October 2004 report on outsourcing and the *USA Patriot Act*, as follows:[12]

> As Jeffrey Rosen has pointed out, the Internet in one sense has strengthened privacy, by increasing the opportunity for anonymity, and in another sense has reduced privacy because every use of the Internet leaves electronic footprints behind. Electronic footprints can be collected and analyzed by strangers. Rosen warns about "the danger of being judged, fairly or unfairly, on the basis of isolated bits of personal information that are taken out of context". What holds true for the Internet applies to databases in general. The result is an incomplete picture which information is mistaken for knowledge. As Rosen notes,
>
> > In an age when disaggregated personal information is centrally collected, widely accessible, and permanently retrievable, private citizens run the risk of being treated like celebrities in the worst sense, vilified rather than celebrated on the basis of isolated characteristics.[13]

What makes the description of a person in today's global data world especially worrisome is that the portrait created is not a portrait of one's true self. Our digital selves, in other words, can hardly reflect our true selves. Analysis of data can create a caricature, but it does not create a person—and the essence of privacy is maintaining your personhood. This is of more than philosophical concern. The pooling of data streams and analysis of the data can have real and costly consequences for individuals.

Intimate information that people once might have shared only with their closest friends now has a way of gathering in secret places for the scrutiny of those with the money or the authority to examine the collective picture. As Charles Sykes has said,

> The very technology that was supposed to free us from mass society and the conformity of mass media has turned out to be as much a fishbowl as an information highway. In modern society, we have discovered that being free means also being naked. The same society that allows us to live anonymously relies on surveillance to keep track of us because we are a society of strangers.[14]

Ten years ago, the Australian privacy expert Roger Clarke coined the term "digital persona" to describe the model of an individual established through the collection, storage and analysis of data about that person. Clarke described the digital persona as a "potentially threatening, demeaning and perhaps socially dangerous phenomenon," especially given the propensity for organizations to employ data surveillance—or "dataveillance", as he called it—to exercise control over the behaviour of individuals and the societies they collectively form:

> If information technology continues unfettered, the use of the digital persona will inevitably result in impacts on individuals which are inequitable and oppressive, and in impacts on society which are repressive. European, North American and Australasian legal systems have been highly permissive of the development of inequitable, oppressive and repressive information technologies. Focussed research is needed to assess the extent to which regulation will be sufficient to prevent and/or cope with these threats. If the risks are manageable, then effective lobbying of legislatures will be necessary to ensure appropriate regulatory measures and mechanisms are imposed. If the risks are not manageable, then information technologists will be left contemplating a genie and an empty bottle.[15]

The contribution of local governments to the proliferation of databases containing personal information cannot be overlooked. The fact that these databases generally contain transaction-related personal information and basic demographic information such as name, address and related data fields does not mean these expanding personal information systems carry no privacy risks. At the very least, they can present privacy risks such as identity theft. More important, taken in combination with other sources of personal information in the hands of state agencies—whether from public or private sources—such databases undoubtedly contribute to growing pools of personal information

available for uses both appropriate and inappropriate in the name of law enforcement and public safety.

The 1977 federal US Privacy Protection Study Commission expressed grave concern about the consequences of automated record-keeping for protection of personal information in relation to even small record-keeping systems:

> The real danger is the gradual erosion of individual liberties through the automation, integration and interconnection of many small, separate record-keeping systems, each of which alone may seem innocuous, even benevolent, and wholly justifiable.[16]

While these might sound like prophetic words, the US Commission could hardly have foreseen the extent to which databanks would be integrated a quarter of a century later. Nor can we predict with any accuracy where technology will take information management in another 25 years. Uncertainty about the future underscores the need to establish sufficient legal privacy protections today so that public policy will guide technology rather than blindly follow it. We also need to ensure that legislative authority is exercised responsibly and sparingly, especially where the legislation explicitly aims to establish personal information databases through surveillance initiatives—and particularly where legitimate doubt exists about the authority to pass such bylaws in the first place.

The dangers inherent in these expanding bylaws and information systems demand a responsible approach on the part of any local government that is contemplating enactment of such a bylaw. Our view is that British Columbia's local governments should not enact bylaws that compel businesses to collect and disclose customers' personal information.

Municipalities have contended that it is necessary to collect this personal information to carry out their role in regulating and licensing businesses, a responsibility assigned under the *Community Charter*. This is not a tenable position. The routine collection of personal information of all customers of specific kinds of businesses, and the routine disclosure of that personal information to police, are not a "necessary" part of the regulation of businesses. These bylaws are instead designed to compel collection and disclosure of personal information to enable the police to monitor the activities of individuals who the police believe may be potential criminals, to determine the whereabouts of individuals suspected of criminal activities or to find people who are of interest to the police for some reason. This undoubtedly allows the police to carry out their activities with greater ease, but it is not credible to say that these bylaws are a necessary part of business regulation. These bylaws smack more of regulating individuals.

Moreover, the impact on the rights of the individuals who are monitored, the vast majority of whom are simply using a completely legal service or buying legal products for innocent reasons, is a matter of considerable concern. It is unlikely

that individuals who deliver secondhand clothing for sale by a consignment shop would expect their personal information to wind up on a nationwide police database, accessible to police agencies across Canada. Nor would they expect that renting a private mail box would result in their personal details being available in police information systems.

This is a real concern because, through software programs and services such as Xtract or Business Watch, police have the ability to monitor citizens whether they are suspected of a crime or not and to share that information with police agencies throughout the country and North America. The original intention of a bylaw such as a pawnbrokers and secondhand dealer bylaw was to ensure that stolen property was not re-sold through such businesses. However, one wonders whether local governments and police agencies see a further opportunity to keep track of individuals through the recording of personal information and its subsequent forwarding to the police. This concern applies also to bylaws relating to activities such as mailbox rentals, sale of pepper spray and sale of hydroponic gardening supplies.

These kinds of surveillance bylaws significantly alter the general privacy landscape. In the absence of any legal compulsion to do so, businesses are not obliged to disclose personal information of their employees, clients or customers to the police. Legal compulsion may involve a legislative disclosure obligation, but disclosure to the police or another law enforcement agency[17] is usually not required unless a court order, warrant or subpoena has been issued to the business.[18] The core attribute of the bylaws under discussion is that they circumvent the courts and their processes, which offer due process and independence from government and its agencies, including the police.

This Office strongly believes that municipalities should not be in the business of passing surveillance bylaws. They clearly have privacy implications of varying degrees, depending on the nature of the personal information being collected, for ordinary members of the public who are going about their lawful business. Among other things, none of the bylaws we saw contains measures to ensure that personal information is used properly and is protected against unauthorized use or disclosure. Against the undoubted privacy impact of such bylaws, it is doubtful that such bylaws are really effective. There are certainly tools that may more effectively achieve the community safety objectives that the bylaws purport to address.[19]

This is particularly the case, in light of the *Safety Standards Amendment Act, 2006,*[20] regarding municipal bylaws aimed at businesses that sell hydroponic equipment and supplies, which may be used in marijuana production. Amendments under the *Safety Standards Amendment Act, 2006*, which came into force in June of this year, require BC Hydro, and other electrical power producers, to share domestic electrical consumption information with municipal safety authorities. This is intended to allow safety officials to inspect residences

whose electricity consumption is sufficiently high over time to identify possible marijuana grow-ops.

It is clear that the *Safety Standards Amendment Act, 2006* provides a much more direct and effective tool for identification of suspected grow-ops than any municipal bylaw aimed at sales of equipment or material that might, just might, be used for illegal purposes. This new law effectively removes the point of such municipal bylaws and municipal councils should, for this reason as well, not be passing them.

In the case of bylaws dealing with pawnbrokers and second-hand dealers, we acknowledge that there is a public interest in preventing the fencing of stolen goods and in recovering stolen property. As noted earlier, the Pawnbrokers Association does not object to bylaws that require pawnbrokers to keep registers of property that they take in pawn and sell, but does not believe local governments have the power to force businesses to provide customer information to police agencies on a regular basis (as opposed to an item-by-item basis on inquiry by the police).

Like the Pawnbrokers Association, this Office recognizes and supports the role of law enforcement agencies in ensuring that property left with such businesses is not stolen. Municipalities should not, however, be passing bylaws that place all citizens who do business with pawnbrokers or second-hand dealers under surveillance in the form of routine disclosures of personal information of all customers. This is especially important because the Court of Appeal has yet to resolve doubt about whether s. 59(1)(b) of the *Community Charter* actually authorizes bylaws that compel collection and sharing of personal information in this way.

Specifically, we strongly believe that municipal bylaws regulating pawnbrokers and second-hand dealers should go no further than to require them to collect identifying personal information of those who leave goods and make that information available to police upon request in relation to specific stolen goods. Such a bylaw would require businesses to collect and retain identifying information. The only information that would be regularly disclosed would be information identifying goods pawned or sold. If goods were matched with stolen property, the personal information of the individual involved would be disclosed by paper or electronic means. This workable compromise may not satisfy all law enforcement officials, but it is a reasonable and justified position, particularly in light of the real and pressing dangers associated with the growth of surveillance databases and systems in our society.

We know that British Columbia communities face law enforcement challenges associated with drugs and related criminal activities. Local government politicians may, we acknowledge, be tempted to pass laws that at least appear to address community concerns. But the efficacy of bylaws compelling businesses to put their customers' information in the hands of police is open to question, to

say the least. Yet, as indicated above, the privacy impacts are clear both in the immediate sense and as part of the overall trend toward more surveillance, which is often implemented without hard questions about balance and efficacy being asked. Local governments that are concerned about criminal activities should not in our view open the statute book without first using other tools to address these problems. A municipality that is committed to assisting with enforcement of the criminal law and the safety and well-being of its citizens will use other bylaw powers first, before passing laws to compel the private sector to create surveillance databases. It will also commit the financial resources necessary for the proper enforcement of all laws, including enforcement of the *Criminal Code*, before passing bylaws that put entire classes of individuals under surveillance and suspicion without grounds.

In conclusion, municipalities should not pass bylaws compelling citizens to give up their privacy in a wholesale and indiscriminate manner. Consistent with long-standing law and practice in Canada, it should be left to the courts to issue warrants or orders to businesses to turn over customer information on a case-by-case basis where justified.

3.0 CONCLUSION

We recognize that, despite the views expressed here, a municipality may decide to proceed with a bylaw. At the very least, any local government considering adopting any bylaw that would compel businesses to collect, compile or disclose customers' personal information for law enforcement purposes should follow these steps:

1. Such a bylaw should only be adopted as a last resort. Other measures ought to be considered before a bylaw is entertained as a solution. A bylaw should be adopted only where conventional means for achieving the same law enforcement objectives are *substantially* less effective than the bylaw promises, on clear evidence, to be *and* the benefits of surveillance *substantially* outweigh any diminution of privacy inherent in the bylaw's operation. The local government should be prepared to demonstrate that these factors have been satisfied.

2. The local government must be prepared to justify the use of a surveillance system on the basis of verifiable, specific reports of incidents of crime, public safety concerns or other compelling circumstances.

3. Before proceeding with a bylaw, the local government should complete a privacy impact assessment ("PIA") to assess the actual or potential effects the proposed bylaw may have on privacy and on the ways in which any adverse effects are to be mitigated.

4. A copy of the completed PIA, together with the local government's case for adopting the bylaw as opposed to other measures, should be sent to this Office for review and comment. We should get these documents well before any final decision is made to proceed with a bylaw.

5. The local government should, before deciding to proceed, conduct consultations with relevant stakeholders—including affected businesses—who may be able to assist in making an informed decision as to the necessity for, and acceptability to the public of, the proposed bylaw measures.

6. The bylaw, if adopted, should be designed so that the privacy intrusion it creates is no greater than is absolutely necessary to achieve the legislative goals.

This document was prepared by David Loukidelis and by Jim Burrows. We are grateful to those who took the time to provide comments to us.

August 30, 2006

ORIGINAL SIGNED BY

_____

David Loukidelis
Information and Privacy Commissioner
for British Columbia

OIPC File No. F03-17823

END NOTES

[1] In recent years, there have been rumours—and at least one media report—that police forces, including the RCMP, have asked municipalities to pass bylaws such as those discussed here, notably hydroponics bylaws. On February 7, 2006, I wrote to Beverly Busson, Deputy Commissioner of the RCMP and Commanding Officer of the RCMP's "E" Division, and asked her to "confirm whether individual RCMP detachment commanders in British Columbia have the discretion to initiate or request such bylaws." I also asked if, assuming this is the case, "there are any policies or rules surrounding their exercise of that discretion, or any Division or overall RCMP policy on such matters". The RCMP's response came in a July 26, 2006 letter from Gary Bass, Assistant Commissioner and Officer in Charge Criminal Operations, "E" Division. The letter did not directly respond, but did refer to co-operation between police and local governments in responding to crime problems.

[2] Apparently mailboxes might be used for criminal activity of some kind.

[3] Pepper spray apparently might be used to assault someone.

[4] The obvious aim of these bylaws is to counter marijuana grow-ops.

[5] This is clearly aimed at hydroponic marijuana grow operations.

[6] (1989) 33 B.C.L.R. (2d) 202 (B.C.S.C.).

[7] This statement does not apply, at least with the same force, to bylaws enacted under s. 59(1)(b) of the *Community Charter*, in relation to pawnshops and second-hand dealers. Earlier this year, the BC Supreme Court decided that s. 59(1)(b) authorized a pawnbroker and second-hand dealer bylaw that compelled collection and disclosure to police of personal information. See *Royal City Jewellers & Loans v. New Westminster (City)*, 2006 BCSC 203, [2006] B.C.J. No. 270. That decision is under appeal at this time. The Court of Appeal will have to decide whether, even if s. 59(1)(b) does authorize a bylaw that prohibits the businesses of pawnbroking or second-hand goods dealing, it therefore "follows that providing such establishments authority to 'notify' the police must go beyond simply providing the police with a description of the goods taken in pawn."

[8] In that decision, Lysyk J. ruled that the City of Vancouver had a legitimate interest in ensuring that escort services did not offer the services of unlicensed escorts and that the personal information was used for verifying compliance with the licensing requirements. Accordingly, a bylaw "establishing rules requiring a person carrying on a business to maintain a record may be found to be *intra vires* [within] the authority of a municipality to regulate, by inspecting, if a record is made for purposes of inspecting to see if there is compliance with the lawful requirement or standard." The UBCM Opinion implicitly appears to recognize this. In its conclusion, the opinion introduces a qualification not stated in the main discussion—it says that any bylaw compulsion to collect personal information would have to be "necessary to ensure compliance with the requirement or standard in the bylaw." In other words, as *International Escorts* indicates, a bylaw requiring businesses to collect and disclose customer personal information is valid only to the extent that the requirement is part of an otherwise valid regulatory scheme or requirement. A stand-alone requirement to collect and disclose personal information would not be valid—the requirement must be ancillary to a valid regulatory scheme. This conclusion is not altered by differences between the *Community Charter* and the *Vancouver Charter*, with which *International Escorts* dealt.

[9] Lower Mainland Municipal Association, Annual General Meeting and Convention (May 10-12, 2006), found at http://www.lmma.bc.ca/pdf/2006_RESOLUTION_DISPOSITION.pdf.

[10] (Unreported, 3 December 2003), New Brunswick (N.B. Prov. Ct.).

[11] This document does not consider whether bylaws that compel collection of personal information and its disclosure to police violate the *Canadian Charter of Rights and Freedoms* ("Charter") and are thus unconstitutional.

[12] Office of the Information and Privacy Commissioner for British Columbia, *Privacy and the USA Patriot Act: Implications for British Columbia Public Sector Outsourcing* (October 2004): http://www.oipc.bc.ca/sector_public/usa_patriot_act/pdfs/report/privacy-final.pdf.

[13] Jeffrey Rosen, *The Unwanted Gaze: the Destruction of Privacy in America* (New York: Vintage Books, 2001) at 200-202.

[14] Charles J. Sykes, *The End of Privacy* (New York: St. Martin's Press, 1999) at 16.

[15] Roger Clarke, "The Digital Persona and Its Application to Data Surveillance", *The Information Society* 10:2 (June 1994).

[16] US Privacy Protection Study Commission, *Personal Privacy in an Information Society* (July 1977), available online at www.epic.org. Similar warnings were sounded earlier in *Privacy and Computers*, the 1972 report of a task force established jointly by the Canadian Departments of Communications and Justice. Also see *Records, Computers and the Rights of Citizens,* the 1973 report of the Advisory Committee on Automated Personal Data Systems established by the US Secretary of Health, Education and Welfare, online: www.epic.org.

[17] Section 26(c) of the *Freedom of Information and Protection of Privacy Act* ("FIPPA") authorizes a public body, including a municipal police force, to collect personal information "for the purposes of law enforcement", which includes policing. Section 27 authorizes a municipal police force to indirectly collect personal information for law enforcement purposes, *i.e.*, to collect personal information from sources other than the individual whose information is collected. Police forces, like other public bodies, can also collect personal information indirectly where authorized by an enactment. Bylaws are enactments as defined in the *Interpretation Act*.

[18] Section 18(1)(o) of the *Personal Information Protection Act* ("PIPA") authorizes a private business to disclose personal information of customers, without their consent, where the disclosure is "required or authorized by law". A "law" includes a local government bylaw.

[19] Section 63 of the *Community Charter* authorizes municipalities to pass bylaws addressing protection of persons and property, including fire safety. Safety standards bylaws may, along with building bylaws, provide municipalities with opportunities for combating grow-ops in conjunction with the powers recently established under the *Safety Standards Amendment Act, 2006*.

Section 64 of the *Community Charter* authorizes a municipality to pass bylaws aimed at protection of the well-being of the community in relation to nuisances, disturbances and other objectionable situations. They can pass bylaws prohibiting nuisances, prohibiting matters that are liable to disturb the quiet, peace, rest, enjoyment, comfort and convenience of individuals or the public, and refuse, garbage or other material that is noxious, offensive or unwholesome.

Last, s. 18 of the *Community Charter* authorizes municipalities to enact bylaws establishing circumstances in which they may discontinue providing a municipal utility or other service to a property or a person, including non-compliance with rules established by bylaw respecting use of the service. A bylaw could provide that a service such as sewer or water cannot be used for unlawful activity, such that breach of the rule would result in termination of the service. The validity of such a rule is open to some question, but this avenue should be explored.

[20] S.B.C. 2006, c. 31.