ANPR: Code and Rhetorics of Compliance

by Christopher Parsons,¹ Joseph Savirimuthu,² Rob Wipond,³ and Kevin McArthur⁴

Abstract: ANPR systems are gradually entering service in Canada’s western province of British Columbia and are prolifically deployed in the UK. In this paper, we compare and analyze some of the politics and practices underscoring the technology in these jurisdictions. Drawing from existing and emerging research we identify key actors and how authorities marginalize access to the systems’ operation. Such marginalization is accompanied by rhetorics of privacy and security that are used to justify novel mass surveillance practices. Authorities justify the public’s lack of access to ANPR practices and technical characteristics as a key to securing environments and making citizens ‘safe’. After analyzing incongruences between authorities’ conceptions of privacy and security, we articulate means of resisting intrusive surveillance practices by reshaping agendas surrounding ANPR.

¹ Christopher Parsons is a PhD Candidate in the Department of Political Science at the University of Victoria.
² Joseph Savirimuthu is a Senior Lecturer in Law at the Liverpool Law School, University of Liverpool.
³ Rob Wipond is a freelance researcher-journalist and sessional instructor in journalism and nonfiction at the University of Victoria and Royal Roads University.
⁴ Kevin McArthur is a web architecture developer who specializes in e-commerce and security research on encryption systems.
Authorities have been invested in tracing the movements of citizens and foreign agents for centuries. Borders between and within states and regions have historically been sites to control and monitor the flow of populations, but only recently have socio-technical and bureaucratic systems “actually developed the capacities necessary to monopolize the authority to regulate movement” (Torpey 2000: 7). While the passport was one of the earliest means of systematically tracking movement, it is licensing systems, often tangibly manifest as identity or driving cards, that are widely used to authenticate and identify citizens and foreign travellers circulating within the nation-state’s borders today (Froomkin 2009). Though passports and other identity cards function as an “expression of the attempt by modern nation-states to assert exclusive monopoly over the legal means of movement” (Torpey 1997: 13), they mustn’t be read in isolation: to track and trace individuals in a systematic manner presumes a hierarchical state with an interest in collating and disseminating information across state organs in a maximally efficient way using standardized communications mechanisms (Lyon and Bennett 2008: 15-6).

The tracking and tracing of individuals in Canada and the United Kingdom (UK) is increasingly facilitated using Automatic Number Plate Recognition (ANPR) systems. Such systems are in trial phases in Canada’s westernmost province, British Columbia (BC), and widely deployed in the UK. ANPR is used to monitor vehicular movements, but the value of the monitoring is realized largely insofar as licensing techniques - predominantly those linking individuals to specific license plates - and policing, insurance, and other third-party databases can be, and are,

---

5 Throughout this paper we commonly refer to this technology as “ANPR”, despite it being termed “Automatic License Plate Recognition” (ALPR) in Canada; adopting the sole acronym is meant to assist with readability.
integrated with ANPR systems. Whereas the track and trace capabilities that were possible at the passport’s inception required analogue investigation of individuals’ documents, and where the investigation of citizens’ vehicular movements previously required significant material and temporal resources on the part of the state, the contemporary linkage of multiple data stores with automated image sensing technologies enables a previously unheralded ability to massively surveil resident and transient populations. Identity card politics have shifted: while the ‘card’ is a physical instantiation of the surveillance apparatus, the icon of the card now rests overtop the massive conglomerated databases that drive and enable ANPR-based surveillance.

In this paper, we unpack how ANPR systems have been deployed, examine their significance, and propose measures to resist and mediate their intrusive surveillance capabilities. We start by discussing how ANPR systems function to instruct the reader about these systems’ potentialities and limitations. We then provide an overview of how the systems are deployed in BC and the UK. This has us focus on the institutional configurations that enable ANPR systems as well as the contemporary dimensions of ANPR systems in these respective jurisdictions. By focusing on both jurisdictions we can engage in brief cross-comparative analyses of ANPR systems. We conclude by offering techniques for resisting the spread of ANPR: how have critics of the technology engaged the political agenda, and what has been entailed in their framing of the technology and its purposes?

What is ANPR?

Automated Number Plate Recognition systems are public surveillance systems, insofar as they involve “the focused, systematic and routine attention to personal details for purposes of influence, management, protection or direction” (Lyon 2007: 14). Law enforcement justifies ANPR-based surveillance by arguing that the system can “improve productivity” of officers and “can be valuable in preventing or solving many types of crime plaguing society” (Gaumont 2008). ANPR systems automatically "extract vehicle license plate information from an image or a sequence of images." Image extraction entails identifying the characters imprinted on vehicle license plates using infrared cameras and subsequently parsing the characters using optical character recognition processes. Successfully identifying plates involves correcting for plate size, angle of image capture, color of the plate and its characters, occlusion, illumination, and other variables. After extracting the characters, the ANPR system may be used for freeway monitoring, be used in conjunction with an electronic payment system (e.g. toll payment, parking fee payment) (Du, Ibrahim, Shehata, and Badawy 2011), or be interfaced with policing and insurance databases for law enforcement purposes. In the course of this paper we exclusively speak to how ANPR systems are used for policing purposes.7

ANPR systems that are deployed by police are typically linked to, or use data associated with, databases that are formally outside of the ANPR systems’ immediate scope (e.g. RCMP 2009,

---

6 Cutting edge research investigates identifying vehicles’ make and model in addition to the license plate (see: Sarfranz and Khan, 2011); in this paper we exclusively focus on current license plate analysis practices.

7 We recognize that insurance and policing are not always directly linked; for our purposes we will speak to cases where law enforcement is involved in monitoring for uninsured drivers. Recent revelations in the United States touch on other insurance-based uses of ANPR: the collection of driving data by authorities and its subsequent disclosure to insurance companies. For more, see Greenberg (2012).
Memorandums of understanding or other legal arrangements are often established so that data from central policing databases containing license plate information, or insurance databases run by public and private insurers, can be drawn into an ANPR-specific “hit” database. In this way a new, ANPR, database is initially loaded with information about specific license plates. These ‘hit databases’ are, in effect, a function-creep consequence of data permeability across databases that were rarely, if ever, designed with ANPR surveillance in mind.

Data records from the ANPR databases are subsequently made available to ANPR sensing equipment, including fixed cameras along major roadways, cameras permanently affixed to authorities’ vehicles, and temporary camera installations attached to either vehicles or built infrastructure. Making data available often entails temporarily downloading information to local data storage equipment (e.g. USB thumb drives, small amounts of memory integrated with the camera sensing equipment) from the ANPR hit database or regional policing databases (RCMP 2009) or, alternately, having an ongoing data link between camera installations and the hit database, where the camera unit possess either live data link or ‘fast track’ capabilities (ACPO NPIA 2009). ANPR systems will typically have two broad definitional categories for plates that are identified using ANPR: “hits” and “non-hits.” Hits correspond to data derived from policing and insurance databases - plates of interest to authorities; non-hits are all other scanned license plates.

Whenever a camera scans a license plate it evaluates whether the plate is a “hit” or not. In the case of a hit an alarm will sound and alert the officer that a plate of interest has been identified by the camera. This analysis and alerting functionality is seen to facilitate “operational readiness” by providing contemporary technologies to policing organizations (RCMP 2009: 18). Policing practices vary at this point but in many cases officers are instructed to double-check the camera’s accuracy before pulling over a vehicle and its driver (RCMP 2009, Lum, Merola, Willis, and Cave, 2010: 2). When license plates are registered by the system they are immediately linked with temporal and geolocational information (RCMP 2009, ACPO NPIA 2009). This geo-temporal information can subsequently be uploaded to the ANPR database and, over time, be used to map movements of persons/vehicles of interest. Some ANPR systems also
enable police officers to ‘live query’ master ANPR databases so that they can see where either hit or non-hit vehicles have been previously sighted (ACPO NPIA 2009, Priest and Arkin, 2011: 141). When integrated with Global Information Systems (GIS) this facilitates profile-building and migration pattern awareness. Consequently such systems can “track observations that may have no criminal connotation alone but which, when correlated, could be suggestive” (Priest and Arkin 2011: 141, see also: Lum, Merola, Willis, and Cave 2010: 70-1). The risk, as will be discussed in subsequent sections, is that over time poor data confidence rates will lead to inaccurate database polling and evaluation which will, in turn, promote highly questionable suggestions of criminality.

State Institutions and ANPR

While ANPR systems generally adhere to the characteristics outlined in the previous section, they can vary somewhat from this general configuration. In this section we explore how ANPR systems have been, and presently are, configured and their relationship with domestic political institutions and conditions. In discussing British Columbia and the United Kingdom we first outline the key actors invested in the ANPR policy networks. From there we discuss how law enforcement authorities, in particular, have sought to marginalize access to information about these systems to defray public insight into the actual practices and uses associated with these surveillance systems.

British Columbia

Deployments of ANPR in British Columbia have been driven by the federal policing force, the Royal Canadian Mounted Police (RCMP). The RCMP are, in addition to federal authorities, also contracted by the province of British Columbia to provide provincial and some regional policing services. ANPR was, and continues to be, an RCMP-driven surveillance process (VicPD 2011). In the course of justifying and deploying ANPR systems they have been in contact with federal and provincial privacy commissioners, and non-RCMP municipal policing forces. The ANPR policy network in BC is thus very small, with only the most limited media awareness of the projects prior to the efforts of locally situated privacy advocates.

The Actors

ANPR was first used in Canada for toll-road applications (Bennett, Raab, and Regan 2003) and then for border management processes (Gaumont 2008: 3). In 2006 the RCMP began using the technology for “traffic and criminal code enforcement” (Gaumont 2008: 3). Per the RCMP’s 2009 Privacy Impact Assessment (PIA) dated from 2009, ANPR systems could eventually be deployed across the entire country (RCMP 2009: 15); such deployment would be solely to address “road safety issues and stolen vehicles” and not “as an intelligence gathering tool” (RCMP 2009: 20). Initial deployments of the technologies captured hit and non-hit vehicular data alike; the former was stored for two years whereas the latter was kept for sixty days. In subsequent updates to the ANPR system non-hit data has been designed to be purged post-

---

8 While there was a 2005 Preliminary Privacy Impact Assessment that was provided to Canada’s federal privacy commissioner for review the RCMP has, to date, failed to release this document to the public.
collection, when it is uploaded from sensing devices to an ANPR collection database (RCMP 2010: 2).

Hit data categories, at the time the PIA was prepared, included the following from the Canadian Police Information Centre (CPIC): Stolen vehicles, Accused Person, Court Action, Missing Person, Parolee, Prohibited Person, Refused Person, Special Interest to Police, Wanted Person. These categories are extensive; anyone with a criminal code offence but who is not wanted on warrant is included, as are persons who have custody of a child as specified by an order of the court, as are persons who have an order of prohibition against them with regard to liquor, firearms, vehicle driving and boat operation, hunting, or any other court or statute imposed prohibition, as are persons police identify as threats to themselves by reasons of an apparent mental disorder. Provincial data is drawn from the Insurance Corporation of British Columbia (ICBC) and includes Unlicensed Drivers, Vehicles with no Insurance, Prohibited Drivers, and Suspended Drivers (RCMP 2009: 37-41). In addition to these database categories, early versions of the RCMP’s 2009 PIA noted that other data elements, such as “race, ethnic origin, gender, blood type, financial transactions etc” were also being, or planned to be, retained in the ANPR database (Office of the Privacy Commissioner of Canada 2009). At a point between the Officer of the Privacy Commissioner of Canada’s (OPC) evaluation of the ANPR program and the final PIA released by the RCMP, all mention of these other data elements were purged, though it remains unclear whether the data was ever, actually, integrated into the database.

The OPC raised a set of concerns regarding the ANPR program. It noted that, despite RCMP statements to the contrary, the ANPR systems would collect Personally Identifiable Information (PII) on the basis that there are links between license plates and identifiable individuals. These links between number and person in databases - as opposed to between the number and a picture of a person - are sufficient to constitute PII. While the Office was concerned about how the new ANPR hit and collection databases would be secured, it was staunchly opposed to the collection of non-hit data; such data was to “be destroyed immediately” upon capturing it “so as to eliminate the possibility of a breach” (Office of the Privacy Commissioner of Canada 2009: 7). Concerns were also raised about the accuracy of retained personal information - a topic that will be addressed in a subsequent section - as well as around access to information. More specifically, the Commissioner recommended that a process that was independent of formal Access to Information and Privacy (ATIP) requests be established so that citizens could ascertain whether their data was contained in an ANPR-related database (Office of the Privacy Commissioner of Canada 2009: 3-8). To date, such an alternate means of accessing stored information has not been established.

The RCMP functions as federal and, in BC, provincial authorities. As a result of their partnership with the province’s sole government insurer (ICBC) and municipal policing authorities, the provincial privacy commissioner was also appraised of the ANPR system. After the Office of the Information and Privacy Commissioner (OIPC) learned about the ANPR system in 2010 it identified several grounds for concern. A municipal policing force, the Victoria Police Department (VicPD), was told that the ANPR system was capturing personal information which stood in contradiction to the department’s “suggestion,” in earlier consultations, that no PII was

---

9 This category concerning Persons of Interest, or those could harm themselves, was entirely redacted in the PIA received by Rob Wipond. Information was supplied during interviews with RCMP staff.
collected. The Office also raised worries about the scope of data collection, because the PIA developed by the RCMP was designed to meet federal, not provincial, privacy law. Consequently the OIPC asked for “a list of the proposed alerts and an explanation for the rationale for the collection” (OIPC 2010: 2). The OIPC also noted that VicPD would have to appraise the office of data retention plans and rationales, as well as a “detailed explanation for any proposed secondary use of personal information gathered” along with an “evaluation of the authorities for such further use or disclosure under FIPPA”\textsuperscript{10} in order to demonstrate compliance with BC’s provincial privacy legislation (OIPC 2010). From documents received under ATIP and Freedom of Information (FOI), it remains unclear whether local authorities responded to the OIPC’s concerns. It is clear, however, that ANPR systems were being purchased before VicPD’s information and privacy manager received responses to the Commissioner’s questions; in one email thread she was advised to not go on television until “those privacy issues” were resolved, a point on which she agreed (VicPD 2010: 46-7).

In addition to this small group - RCMP, VicPD, and federal and provincial privacy commissioners - there was a smattering of media coverage on ANPR, typically praising its general effectiveness. Significant media attention to the technology began in early 2012 with the publication of two magazine articles critical of ANPR (Wipond 2012a, 2012b) and an academic presentation on BC deployments of ANPR (Parsons, Wipond, McArthur 2012). With the OIPC’s mid-2012 announcement that they would formally investigate ANPR deployments in BC a swathe of national media coverage arose. This coverage led to privacy advocates and policing bodies being routinely quoted in media about the threats and merits of the technologies.

The recent media interest in ANPR is largely the result of ongoing research by three civil rights advocates located in BC. The BC group is composed of an advocate/journalist who has conducted interviews, written articles, and submitted ATIP and FOI requests (Rob Wipond), an advocate/researcher located at the University of Victoria (Christopher Parsons), and an advocate/technologist that is actively invested in digital privacy and security issues (Kevin McArthur).\textsuperscript{11} Their efforts have been supplemented by long standing civil rights groups throughout BC who have provided legal and strategic assistance, though these three are the principles on this issue in the advocacy community in BC.

Marginalizing Access

Canada, like most other Western nation-states, has laws to secure citizens’ personal data from unjust or non-consensual collection, use, and disclosure. These laws and associated Privacy Commissioners, while somewhat less comprehensive than EU privacy and data protection laws (Newman 2008), are nonetheless regarded as “reasonably effective” despite not being perfect (Flaherty 1999). Deeply associated with provincial and federal privacy legislation are access to information laws. Such laws are intended to force the disclosure of information to the public and thus act as a control on government generally (Burkert 2007) though, as documented by Gilbert (2000), secrecy is a pervasive aspect of the Canadian Westminsterian system. Access to information legislation in fact has led to the cessation of some record keeping, primarily of

\textsuperscript{10} FIPPA stands for “Freedom of Information and Protection of Privacy Act”, and is BC’s provincial privacy law.

\textsuperscript{11} The description of these advocates - advocate/researcher, advocate/technologist, and advocate/journalist - is taken from Bennett (2008).
deliberations and meetings, so as to avoid creating document trails that could subsequently be disclosed to the public.

Journalistic interviews were repeatedly conducted with ATIP and FOI officers working for policing forces in Canada, and have regularly been stymied by efforts to mislead or flatly deny the existence of ANPR-related documents. Rather than detailing all of these encounters, a small sample are provided of multiple encounters. At the municipal level, researchers contacted the VicPD and filed a request for all documents of all types pertaining to the ANPR system. The Information and Privacy officer stated that “We actually don’t have a program … Everything goes through [the RCMP]. We don’t have documents per se. Everything, we receive everything from them. It’s on a USB stick.” When a followup question was asked to confirm that there were no documents, no email, or other correspondence about the program, the officer stated that they would “do a little more research and hopefully there’s some kind of administration [sic] paper trail.”12 Days later the officer responded that they had found “the policy, I have board minutes, I have some emails between the RCMP and myself … I have 2 years of emails here.”13 In the same interview, the officer insisted that there was “no bullet here” and that all the communications reflected positively on the program. When all was told, over 700 pages of documents were disclosed. On inspection of the documents, it was evident that the officer was either the recipient or author of a great majority of the ANPR-based communications. As a trained professional the officer had, in our opinion, apparently sought to mislead us, from the beginning, about their possession of documents. This was just one of many efforts to marginalize information to a system that we know, from their own correspondence, was something that might have “privacy issues.”

The municipal authorities, however, are not administrators of the ANPR programs. Their ANPR-outfitted vehicles are used to identify vehicles and store locational surveillance information, but data is downloaded from an RCMP-controlled hit database and uploaded to other, also RCMP-controlled, collection servers at the end of shifts. Our efforts to access information from the RCMP have largely been stymied; the initial access request was for all documents, memoranda, reports, and correspondence related to the ANPR program. RCMP ATIP officers have routinely sought to force a reduction of the scope of the request while refusing to assist in limiting this scope. As an example, after we asked for email messages, an ATIP officer stated “with our system [sic] emails are kept only for 90 days. And unless you give us specific names of employees, we won’t be able to search for emails in regards to the ALPR system. Unless they were filed into specific files, or you give us specific names of employees. So we wouldn’t be able to search for emails.” A follow-up question, “Is that legal?” was met with “[slight laugh] I’m just telling you what happens.”14 This server-based email retention policy limits access to communications by simply not automatically storing them beyond a 90-day period. The requirement to narrow searches to specific officers when researchers are unlikely to know who is involved in specific projects further undermines their capability to learn about these projects. While some RCMP officers retain records beyond the 90-day policy there is no standard retention policy that we were provided with. Without a clear guide or policy around email record

---

12 Interview with VicPD Information and Privacy Manager, September 2, 2011.
13 Interview with VicPD Information and Privacy Manager, September 7, 2011.
14 Interview with RCMP ATIP officer, Nov 10, 2011.
retention it is challenging, at best, for the public to request access to information insofar as the conditions for its very existence are unclear.

Assistance is mandated under Federal Access to Information laws. The RCMP have been reminded of this requirement by the Information Canada (OICC 2012) in light of formal complaints concerning their intransigence in responding to ANPR-related ATIP requests. RCMP have simply stopped, refused, ignored, or improperly closed access requests related to the ANPR system; the Information Commissioner has noted the impropriety of such actions.15 To date, well over a year after the first ATIP request was sent to the RCMP, only a handful of documents have been received, and only 2 are documents that are not publicly available. No email, memos, or other policy briefings have been disclosed. Most documents pertaining to RCMP involvement in ANPR programs have come through third-party sources, such as the VicPD and the OPC.

These are but three of dozens of ATIP challenges that researchers have encountered with authorities, and they speak to a willingness by government ATIP officers to marginalize access to government documents. While some scholars see access and privacy laws as legitimizing surveillance practices (e.g. Lyon 2007, Rule 2007, Haggerty and Ericson 2007) in our experience such legitimization is marginal: these laws have been rhetorically, as opposed to substantively, actualized by BC’s provincial, or Canada’s federal, policing body. As noted in the preceding paragraphs, it should be apparent that the Canadian experience around ANPR demonstrates not freedom of information: it demonstrates a governmental fear of releasing information to the public.

United Kingdom

ANPR systems have been used in the UK since 1990 by law enforcement. It was initially confined to gathering intelligence with a view to policing serious and organised crime. The rationale underpinning its present value is that all available methods for detecting and investigating crimes should be employed where criminals rely on vehicles to perpetrate criminal activity. During the last decade the Government and private sector have invested heavily in fixed and mobile surveillance technologies (Home Office 1994). ANPR systems are now an integral part of modern operational policing activity (Gill et al. 2005); local police forces use the cameras to track stolen and uninsured vehicles as well as to tackle serious and organised crime and threats posed by terrorism.

The ANPR system is part of the Police National Computer (PNC) network. The PNC provides a national intelligence database which, in addition to ANPR generated data, includes search engine functionalities to identify known suspects, provide details of vehicles, and map criminal incidents and patterns (NPIA 2010a). ANPR “hits” that are transmitted to the National ANPR Data Centre (NADC) are cross-referenced with datasets in the PNC. If a match is generated (e.g. Stolen vehicle or vehicle used in a robbery) an alert is immediately sent to an officer monitoring the system. Data held in the NADC is provided by police forces and it is estimated that the national ANPR network generates, on average, 16 million real time ‘reads’ each day. The National Policing Improvement Agency (NPIA) has acknowledged that some local forces have

15 Correspondence with the Office of the Information Commissioner of Canada, March 29, 2012.
arrangements with local authorities and private sector organisations to jointly operate ANPR cameras for criminal detection and investigation purposes only (ACPO NPIA 2009).

The Actors

The NPIA has primarily responsibility for the Police National ANPR Programme in England and Wales (NPIA 2010b). The agency delivers the Association of Chief Police Officers (ACPO) Strategy on ANPR (ACPO 2010). Oversight for implementing the strategy resides with its principal stakeholders, which include the NPIA, ACPO, the Association of Police Authorities, the Serious Organised Crime Agency, and the Ministry of Justice (ACPO NPIA 2009). Police forces have access to the NADC upon signing the Memorandum of Understanding, which sets out duties and obligations relating to access and use of the information. In addition to overseeing the development and management of the Programme, the NPIA also provides police forces with guidance on managing and using information in the database. The Agency works closely with the ACPO and the Information Commissioner’s Office to ensure that privacy concerns are addressed at operational levels. The widespread use of ANPR and CCTV technologies across the public and private sector has raised concerns about potential misuse and discrimination as well as about the lack of a coherent strategy towards the applicable processes for transparency, accountability, and compliance (EVSA 2011). Whilst all “data controllers” are bound by the 1998 Data Protection Act (DPA), the lack of a statutory framework regulating ANPR raises concerns about the extent to which ANPR data is being retained, used, and shared across the various operators.  

The data held on the NADC is owned by individual police forces. As the identification of the car and individual by the vehicle registration mark (VRM) constitutes personal identifiable information, data controllers are under an obligation to comply with their responsibilities under the DPA 1998. Subject access requests are processed by the Data Protection/Freedom of Information Offices within local police authorities. Given the extensive use of information captured by ANPR systems, and sharing arrangements between police and other agencies, there is a public perception that retention practices, use of “reads” for the Driver and Vehicle Licensing Agency (DVLA) auditing, and sharing information for detection and investigation, operate outside the safeguards provided by the DPA 1998. 

---

16 The surreptitious use of surveillance technologies must be in accordance with the law and be proportionate: European Court of Human Rights, Kennedy v. The United Kingdom (Application no. 26839/05) (2010), paragraph 124. Note that following the passing of the Treaty of Lisbon, Article 16 of the Treaty on the Functioning of the European Union (TFEU) identifies protecting personal data as a fundamental right. Accordingly, the Treaty covers the processing of personal data by the private and public sectors.

Marginalizing Access

If we view data generated by ANPR as a form of “algorithmic surveillance” that is driven by the logics of contemporary policing, it should not come as a surprise to discover that citizen access to information about ANPR depends on bureaucratic processes.¹⁸ ACPO’s ANPR strategy and policies for rationalising the flow of information not only shapes how police forces view such data, but also how the forces frame the scope of the legal rules for accountability and access.¹⁹ It is in turning to how ANPR data is categorized as ‘intelligence’ in the UK that marginalization is most evident. Specifically, in what follows we discuss the case heard by the Information Tribunal in Mathieson v IC & Devon & Cornwall Constabulary (EA/2010/0174) to unpack how access requests are stymied. The complainant in this case requested, under the Freedom of Information Act, disclosure of the location of ANPR cameras and CCTV cameras with ANPR functionalities operated by the Devon & Cornwall Constabulary. The request was turned down on the grounds of national security (s. 24) and crime prevention (s. 31). What is interesting here is not the classification of the specific data generated by the use of ANPR surveillance technology; the very location of the devices was identified as being a matter of national security and crime prevention intelligence. The ICO upheld the refusal notice on the grounds that the public interest justified nondisclosure. Mathieson’s appeal to the Information Tribunal was successful. The Tribunal agreed that use of ANPR as intelligence tool engaged s. 24 and 31, but made some pertinent observations justifying non-disclosure:²⁰

There is also a clear public interest in citizens being able to judge whether the police are using this technology in the most effective way. Thus, there were (and are) legitimate and important issues for public debate (a) as to whether the APNR system should be used at all; (b) if so, as to where cameras should be located and whether (in general) their location should be public knowledge or not; and (c) as to whether “read” data should be retained at all or, if so, for as long as two years and as to what use should be made of them…

In particular, the general debate about whether it is better for the location of fixed ANPR cameras to be completely open and provide a so-called “ring of steel” or scattered (and relatively covert) is still one that can be pursued without the public knowing the precise location of the cameras; and there is no evidence that the Respondent was in fact using the ANPR system improperly, for example to focus wrongly on a particular community.

The key point here, as the House of Lords Select Committee on the Constitution (HoL SCC) was at pains to stress, is that any use by the State of surveillance technologies and personal information must be preceded by demonstrable evidence that the effects on privacy have been
taken into account. Moreover, it must be proven that such privacy-invasive practices “are proportionate to those objectives” (HoL SCC 2009: para. 69). At present there is an inability to learn where data is collected, thus limiting citizens’ awareness of the extent of state surveillance. Such surveillance, and subsequent use of personal information, can undermine privacy and limit the freedom of the individual (OSC 2006: para. 14.2). The potential intrusiveness of ANPR technologies should not be underestimated, particularly as the data generated can be processed, shared and used by a wide range of actors without effective regulatory oversight. Further, the Tribunal’s suggestions that not knowing where cameras are located does not detract from public discourse is only academically accurate. As scholars of agenda-setting and public policy literatures have written about, abstracted harms are remarkably harder to capture the public imagination than programs that clearly relate to the public’s daily business (e.g. Soroka 2002, Birkland 1997, Cobb and Ross 1997): discussions of ANPR remain largely abstract when the public doesn’t know where the cameras are located. Consequently, such abstracted discussions of ANPR have a more limited capacity to capture the public - and media’s - attention than a more concretely grounded discussion.

Existing practices - and access conditions - may be mediated in light of the recently passed Protection of Freedoms Act 2012. Specifically, it may lead the newly created office of Surveillance Camera Commissioner and the ICO to create a coherent process that brings public and private ANPR operators within its remit. While the ICO has begun this process and indicated that it has been working with police authorities to ensure that ANPR data is deleted after two years (ICO 2011: 11), truly improved access conditions have yet to be realized; UK citizens are still hindered in their ability to learn about deployed ANPR systems. The ICO's efforts may be assisted by the evolving privacy landscape which regulates the overt and covert use of surveillance technologies; Article 16(1) of Treaty on the Functioning of the European Union (TFEU) and the Code of Practice on CCTV and ANPR, as required to be introduced by section 29 Protection of Freedoms Act 2012 will create a transparent and accountable infrastructure for the collection, processing use of personal information by surveillance technologies. It remains unclear, however, what specific and tangible avenues are, or will be, made available in view of the Surveillance Commissioner's participation in a regulatory space previously assumed by the ICO.21

State Framing of ANPR

Both the Canadian and UK governments have been deeply invested in framing ANPR. Their efforts have included redefining or articulating what constitutes personally identifiable information, justifying the social sorting of the population, and being overly suggestive of the accuracy of the ANPR systems that are deployed. Combined, this framing can be understood within a tactical game meant to justify the technology and set media agendas that are essential to quelling or inciting public interest in state programs.

Personally Identifiable Information

Under Canadian privacy law, numbers that are correlated with, or proxy for, broader biographical information are considered personally identifiable information and thus deserving of protection (Kerr 2009: 349-351). This means that license plate information, social insurance numbers, and numbers associated with RFID tags have privacy expectations associated with them; that the number is, or isn’t, publicly available does not mean that it is non-deserving of protections. In the case of license plate information, however, policing authorities have expressed mixed messages.

The RCMP’s PIA varies in its depiction of license plate information: in some cases it is seen as deserving protections and, at other times, it is not (Wipond 2012a). Federal and provincial privacy commissioners have warned authorities that license plate information is, in fact, deserving of privacy protections; however, these warnings have (at best) been minimally integrated into policing discourses. In interviews with RCMP officers who operate the program, we were told that “you don't own your license plate. Your license plate is owned by the jurisdiction that issues it … that image of the license plate or the image of your car are in there, neither of which are personal, because you're in a public place, and the courts have consistently ruled there's no expectation of privacy in a public place.”

It was only after extensive discussions with RCMP staff that we were formally informed via letter that the RCMP does consider license plate information PII, though this has not prevented other officers from publicly stating that the plates are neither private or personal. Even after we’d received official notification from the RCMP declaring license plate data to be PII, Superintendent Denis Boucher, the head of the RCMP’s traffic services, stated publicly that “all we do is identity the hits. There’s no personal information in the ALPR system. It’s merely the license plates” (CBC 2012a). In discussions with members of Canada’s privacy community, we have learned that the RCMP often adopts a contextually situated understanding of PII: when authorities are collecting it the information is not acknowledged as personal, whereas when members of the public or other government agencies request access to the information it is classified as personal to prevent its disclosure.

In the UK, the DPA 1998 is “technology neutral” insofar as it applies to all forms of technologies that process PII. Accordingly, the DPA 1998 imposes obligations and responsibilities on the data collected via mobile and fixed ANPR cameras (Larkins). Given that ANPR data constitutes ‘personal data’ under the Data Protection Act it is incumbent on local police authorities to have clearly defined policies that address information collected by ANPR systems (ACPO 2011ab). Additionally, given that ANPR systems collect personal information about individuals engaging in private activity, the collection of this information potentially engages Article 8 European Convention of Human Rights (ECHR). Consequently, obligations are placed on “data controllers” for two reasons. First, because the free flow of information and pursuit of legitimate

---

22 Interview with RCMP officer, December 22, 2011.
23 Correspondence with RCMP, July 6, 2012.
24 More specifically, data controllers are obligated to adhere to principles such as fair and lawful processing; processing for limited purposes; that the data collected is adequate, relevant and not excessive; retained for clearly defined period; processed in accordance with the rights of the individual; accuracy and security. Individuals can make subject access requests for personal information held by the local police force.
goals on the part of the State and its organisations do not invariably trump individuals’ privacy rights (Article 29 Working Party 2001: 3). Second, because privacy can be regarded as a public good we must recognise that the trade-off be subject to complex governance processes (i.e. Data Protection Act 1998, Article 8 ECHR, National ACPO ANPR Standards 2011, NPIA Practice Advice on the Management and Use of Automatic Number Plate Recognition) and include a wide range of stakeholders.

In turning to an example we see how, despite engaging ECHR A. 8, PII can be collected by ANPR systems to preserve public order. Specifically, the Administrative Court in the High Court of Justice recently held that retaining ANPR-linked PII about an individual participating in public protests for policing purposes may not engage Article 8 ECHR (Catt v Association of Chief Police Officers and Commissioner of Police of the Metropolis [2012] EWHC 1471 (Admin)). Lord Justice Gross’s position, that the plaintiff did not have a reasonable expectation of privacy and that Article 8 was not engaged, emphasised three features: first, the plaintiff had closely associated himself with a protest groups in public and with a significant history of violence, disorder and criminality; second, the police response was proportionate and consistent with the public duty to maintain public order; and third, the policing activity was overt.25

Taken together, we see that the RCMP have a variable conception of whether licensing information constitutes PII and that, in the UK, collection of PII might not engage ECHR protections. In both cases the collected data is used to monitor and take action against specific citizens, citizens who are often frustrated or unable to discern how or why ANPR systems are used to mediate citizens’ actions. This is significant, insofar as strong PII protections could (though wouldn’t necessarily) restrict the use of ANPR systems and their associated practices where the systems and practices infringe on legally protected rights and actions. To avoid such restrictions the basic operations of ANPR systems have been framed as either not involved in the collection of PII or the collection of PII has been justified despite of prospective ECHR protections.

Social Sorting

State framings of PII, in combination with intransigence in making information of these systems available to the public, has the effect of limiting citizens’ concern or awareness of ANPR surveillance. These efforts do not, however, constitute the full efforts of state framing; the state also attempts to frame its social sorting linked to ANPR so as to make it palatable and acceptable to the publics that are surveilled. Both Canadian and UK authorities have identified ANPR systems as enforcement tools that also are valuable for intelligence processes. While RCMP uses of ANPR are stated as just enforcement-based, that position is contradicted by claims that ANPR could be used to evaluate alibis (Shaw 2012) and used more generally for investigative practices subsequent to criminal acts having been committed (Graham 2012). The UK situation has seen ANPR used to limit protests based on broader police surveillance (Evans and Lewis 2012, Parsons 2009) as well as to conduct more general police enforcement actions (e.g. assigning fines/arresting individuals with outstanding license-linked crimes). In what follows we discuss Canadian and UK definitions and framing of who is monitored by ANPR and how articulations of social categories mask broader civil rights concerns.

25 Lord Justice Gross at paragraphs 61-64 http://www.bailii.org/ew/cases/EWHC/Admin/2012/1471.html
Information that has been disclosed in BC about ANPR to the public, to municipal policing bodies, and to provincial privacy commissioners show only seven ‘hit’ categories: stolen plates/license plates associated to stolen vehicles, license plates associated with warrants (Canada Wide), license plates associated to warrants (BC wide), license plates associated to other pointer vehicles, license plates associated to prohibited drivers, license plates associated to unlicensed drivers, and license plates associated to uninsured drivers (RCMP “E” Division; CBC 2012a). This range of categories stands in variance from the thirteen categories listed in the RCMP’s PIA, with many of these categories compressed into the “other pointer vehicles” category. This category captures individuals such as parents with custody of children, those with prohibitions against firearms and boat operation, and so forth. Officers may not have standing to pull over pointer vehicles; they must first “ensure there are valid grounds for conducting a vehicle check” (RCMP “E” Division).

Simply being present in the database is not reason enough for authorities to take action against a vehicle or its occupant(s). This is significant insofar as authorities publicly assert that ANPR systems are used exclusively for enforcement actions: where ANPR systems are used to monitor movements this clearly shifts into intelligence gathering. Municipal police who are embroiled in defending ANPR systems in BC have repeatedly asserted that the technology “can help officers stop prohibited drivers, drivers without insurance and recover stolen vehicles” (Nuttall 2012) though, when asked to identify the full range of what constitutes a hit in RCMP databases, officers have struggled to fully explicate database categories (e.g. CBC 2012a). The inclusion of a swathe of differing categories within “pointer vehicles” has the effect of assuaging public concerns by convincing the general public they are not a “hit” and so not being tracked. One municipal police chief has gone so far as to assert that “It's that old adage, if you haven't done anything wrong and there's no issues, what's to be worried about? If you are on the run from the law or wanted in another province, a prohibited driver, a list of things, and you're associated to a motor vehicle, then you should be worried. I say, you've got to deal with it” (Derosa and Shaw 2012). The washing over of “a list of things” is problematic because it establishes a misleading frame of ANPR’s public appropriateness: while the monitoring for some, such as prohibited drivers, might seem appropriate to the public, the monitoring of others, such as those with legal custody of children, would arguably be less appropriate to the public.

In the UK, a listing of the ANPR database categories are included as part of the NPIA’s guidance document for ANPR (ACPO NPIA 2009). The document is not protectively marked; this varies from the RCMP’s PIA, which was so marked. Per the guidance document, we learn that ANPR operators will see three markers. Each marker possesses a set of options that are intended to influence how officers interact with a vehicle operator. The first marker addresses actions that officers are to take, and include stop, silent (not to stop for routine checks), intel (the vehicle may be stopped if additional grounds exist), and do not stop (for reasons of officer safety or investigative requirements). The second marker can have up to three options set, drawn from the categories of nothing known, firearms, weapons, violent, or fails to stop. The third marker offers reasons for the vehicle’s detection by the ANPR system, and includes drugs, crime, disqualified, docs, drink drive, sexual, other, protest, VISOR, no stop, and intel. These markers are linked to the Police National Computer Identifier, which itself classifies individuals of interest as follows: firearms, explosives, fails to stop for police, weapons, violent, suicidal, mental, escaper, drugs,
contagious, alleges, ailment, offends against vulnerable persons, sex offender, female impersonator, and male impersonator. Beyond the categorizations of the database there is no information, in the guideline itself, describing how broad (or narrow) these classifications are.

Similar to the BC case, simply being in the database is not reason enough for a vehicle to be stopped. Moreover, “storylines” have been developed in the UK to justify the massive expansion of ANPR cameras. Project Champion, as an example, was described to the public as a means of combating police crime and antisocial behaviour but, it was discovered, was actually intended for counter-terror purposes (Walker 2010). Authorities mislead the local community that the cameras were meant to surveil to the detriment of policing the community, with a review of Project Champion acknowledging that the operation “set relations back a decade” (Thornton 2010: 47). The covert nature of the Project fits within the UK’s usage of ANPR for intelligence gathering purposes. The gathering of such information, in tandem with it’s often secretive or opaque use, raises considerable civil liberties and freedoms concerns, insofar as individuals’ privacy is infringed for hidden or unknown reasons. Moreover, many of the categories in both the UK and BC cases speak to a significant broadening of what police might demonstrably need information about: in the Canadian case, is there a demonstrable need for authorities to monitor the whereabouts of parents who have legal custody of their children and, in the UK scenario, must protesters be tracked? In both nations the database schemas, when combined with mass surveillance technologies, facilitate a broad social sorting and surveillance of the population. While, as we discuss shortly, some uses of the technology to address serious crimes might be warranted the use of the technology for monitoring less serious - and sometimes non-criminal - vehicular and personal behaviours is profoundly disturbing.

**Accuracy and Security**

While the relative obfuscation of “what constitutes a hit” is significant insofar as it can significantly shape public and media perception of surveillance systems, ANPR discourses rest firmly atop the notion that, overall, the systems are efficient and effective. Data that has been accessed, either through public or access to information regulations, often suggests high degrees of relative accuracy. In what follows we offer a theoretical model to discuss why what appear to be highly accurate systems are, in fact, grossly imprecise.

Some ANPR systems claim to attain up to a 95% accuracy rate in reading license plates. However, a confidence rating is a much more important and relevant measure of system effectiveness for a complex data collection system of this kind. To the best of our knowledge, no actual, functioning ANPR system has ever been audited and evaluated for its confidence rating. The accuracy rating, meanwhile, is fundamentally misleading.

Consider, for example, a 95% accurate ANPR system operating where there exists a theoretical criminal population of 1% linked to license plates. In the average person's mind, this presents an image where within any 100 plate reads, there would be 1 accurate hit, 94 accurate non-hits, and 5 inaccurate reads. However, this is already a grossly misleading picture. The key issue is that, in the absence of manual checking of literally every plate read, we do not know which 5% of reads are inaccurate. So here is what our data actually look like:
There are an unknown number of instances where a non-hit plate has been misidentified as a different non-hit plate.

There are an unknown number of instances where a non-hit plate was misidentified as a hit plate.

There are an unknown number of instances where a hit plate was misidentified as a non-hit plate.

There are an unknown number of instances where a hit plate was misidentified as a different hit plate (i.e. mixing up a plate linked to a homicide to one linked to an uninsured driver).

When trying to develop a confidence rating, these problems are then compounded and confounded by the types of data storage policies any particular ANPR system is operating under. We need to know, for example, the following:

- In a hits-only storage system, what percentage of hits were manually checked? (e.g. were all hits on "other pointer vehicles" checked, or only those hits leading to actionable responses, like prohibited drivers?)
- In a system that stores both hits and non-hits, what percentage of each were manually checked?
- In either type of storage system, though some percentage of hits or non-hits may be manually checked, does the officer in the field performing the manual check actually have access to the database to make any corrections? (e.g. in BC, police officers in the field currently have read-only access and thus no ability to correct the automated storage of data even when they identify ANPR system misreads.)

In light of all this, an ANPR "accuracy rating" is often a smokescreen that obfuscates the hard numbers needed to produce a confidence rating. In the final analysis, however, one fact is clear: Given the low percentage of hits and actionable hits relative to non-hits, the instances of accurately identified criminality (1%) in our theoretical scenario will be far lower than the instances of misread plates (5%). This is almost certainly typical of most real-world ANPR scenarios. Therefore, it is expected that the objective confidence rating for any ANPR system will be very weak; only a values-based dismissal of the significance of ever-growing amounts of incorrect and questionable records of personal information can ever make up for these technical weaknesses associated with ANPR systems.

Some ANPR systems will upload hot and non-hit data with geo-temporal information to centralized databases. Given accuracy and confidence ratings this can, over time, lead to highly ‘polluted’ databases, insofar as license plates may be massively misidentified over time. The rapidity at which pollution happens - and its automatic nature - speaks to how ANPR systems are radically different from “analogue” processes to investigate vehicles and their occupants. This difference was noted in Bruce Schneier’s analysis of ANPR when he wrote, “Wholesale

---

26 It has been noted by UK police that certain driving patterns adopted by criminals weaken ANPR read effectiveness; this is one example of how accurately identified criminality might be lower than the actual criminal population. For more, see Kelly Fiveash (2012). “Number-plate spycams riddled with flaws, top cop admits,” The Register. Published August 9, 2012. Last accessed September 2, 2012. Available at: http://www.theregister.co.uk/2012/08/29/anpr_riddled_with_flaws_admits_police_chief/
surveillance is not simply a more efficient way for the police to do what they've always done. It's a new police power, one made possible with today's technology and one that will be made easier with tomorrow's. And with any new police power, we as a society need to take an active role in establishing rules governing its use. To do otherwise is to cede ever more authority to the police” (2004). Indeed, the power afforded by ANPR systems is used by some officers to increase their capacity to increase intelligence on individuals, even in the case of false negatives. As documented by Priest and Arkin, some officers recognize that “[e]ven if the pullovers were false alarms, at least they provided a chance to enter more data” (Priest and Arkin, 2011, 143). Consequently, the inaccuracy of these devices is understood as simultaneously enhancing security vis-a-vis greater intelligence gathering regardless of whether a vehicle or its presumed occupants have been properly identified by ANPR-based systems.

Hubbard (2008) warns that collected ANPR-data constitutes an appealing target, not just for hackers who are interested in subsequently using or selling the information, but also for law enforcement officers who inappropriately access and utilize collected information. Based on recent reports from the United States, insurers and repossession companies must be added to the list of parties interested in ANPR databases (Greenberg 2012, Roper 2012). These concerns about who can access data records arguably parallel those associated with any large database of PII. Froomkin suggests that western Europeans “tend to see these pathological uses of identifications systems as just one of many results of a deeper and broader political or social pathology … one gets the sense the western European answer to common-law paranoia about ID card systems would be that if a regime is using ID cards to oppress its people, the problems are much more fundamental” (Froomkin 2009: 257). Though ANPR is distinguishable from a formal ID card, it operates on a similar logic: the tracking and tracing of individuals across large swathes of state-controlled territory by way of surveillance, database integration, and GIS mapping capabilities. While adopting a risk-management solution is typically what is called for in the face of data breach and misuse potentialities, we suggest that, instead, an alternate approach that enables enforcement actions while removing risks of hacking, inappropriate access, and poor ANPR confidence ratings.

Resisting and Mediating ANPR

Resisting and mediating the worst elements of ANPR systems is challenging, with challenges linked to the rigidity of the policy networks in question and the deployment states of the technology. New entrants to the policy network must demonstrate “that there is indeed a problem to which one’s solution can be attached” and recognize that ‘simply’ trying to change settled indicators that register problems constitutes a problem: such modifications challenge the configuration of the regulatory system itself (Kingdon 2003: 92-3). Linking policy events – such as typical policy discussions amongst ‘normal’ actors – with highly symbolic behaviors – instances of violations of principles that infringe on sacred values or stated and respected principles – can let policy issues and the parties advancing them rise to the agenda by focusing attention on issues that would otherwise be left to languish. Success in focusing attention often depends on whether efforts correlate with a focusing event. Such events are “sudden, relatively rare, can be reasonably defined as harmful or revealing the possibility of potentially greater future harms, inflicts harms, or suggests potential harms that are or could be concentrated on a
definable areas of community of interest, and that is known to policy makers and the public virtually simultaneously” (Birkland 1997: 22 (emphasis added)).

Moreover, as soon as an issue is made public new entrants who assume the role of policy entrepreneurs must develop and grow their base. Typically, this kind of work entails connecting “a problem to cultural assumptions about threats, risk, and humans’ ability to control their physical and social environments” (Cobb and Ross 1997: 5). Moreover, these connections must be seen as vibrantly important to regulators, politicians, and the public in a very visceral sense: statistics, nebulous harms, and far-off problems are often insufficient to capture and shape an agenda. As a result, advocates of novel agenda items or processes will tend to more successful if they have “plausible research results and a highly visible, tangible, and dramatic event on his or her side” in contrast to “an advocate with only evaluation data” (Birkland 1997: 134). Strategically, then, we can expect non-established actors to search for focusing events or analogies that give resonance to their issues.

In turning to the BC advocacy experience, these theoretical moves were implemented. As relatively new entrants to the policy network associated with ANPR, they sought to demonstrate that there was a problem - a system of mass surveillance that was under-explored - and a solution - the cessation of data collection could occur while simultaneously enabling ANPR for enforcement actions. Strategically, the advocacy entailed linking actual surveillance with symbolic upsets: the monitoring of vehicles with the sanctity anonymous vehicular movements. While there are strong legal cases to preserve such freedoms, the fact that many individuals drive and they could plausibly be in the ANPR hit database meant that issues could be linked to policy experts and ‘regular citizens’ alike. Moreover, given authorities’ public statements they want to retain non-hit data (CBC 2012ab), all drivers regardless of their legal status could be affected by the surveillance regime. While advocates did communicate in brief with members of the policy network in the months before publicizing their research, full research findings were made available to the public and members of the policy network simultaneously. This mean that both groups - the public and the network - were forced to react simultaneously. The history of ANPR in BC, as well as potential uses, were important in catalyzing concern around the program and have led to formal investigations of the program by the BC Information and Privacy Commissioner.

In addition to identifying ANPR as a problem and publicizing its long and hidden history, advocates have recently suggested their own solution. This solution would let authorities use ANPR for enforcement practices but not intelligence gathering. This, admittedly, could be challenging to successfully mimic in nations such as the UK that have a long history of using ANPR for enforcement and intelligence gathering. Indeed, the strong linkage of ANPR surveillance to national security has meant that even knowledge of where cameras are located are kept from the British public’s knowledge. Unlike the UK experience, intelligence gathering is not ostensibly a core driver of ANPR-adoption by Canadian authorities, thus affording rhetorical space to find (somewhat) common ground.

Successful resistance in terms of ANPR has revolved around a set of best practices that, if enacted, would reduce the dangers to citizens, ameliorate surveillance-related concerns, and maximize confidence ratings in retained data. Under the best practices and data flow model
below, authorities can continue to use ANPR and citizens can be assured that a database of their movements not being automatically aggregated or that this data is being used for unknown purposes post-collection.

**FIGURE 2: Enforcement-Based ANPR Data Flow**

Under our model the ANPR system would not retain any data: all collected data would be the result of normal policing records that follow a traffic stop/investigation of a vehicle. Consequently, tertiary databases - such as the ANPR collection database shown in Figure 1 - would not develop or exist. The ideal way for using ANPR for policing enforcement processes, while maximally alleviating civil liberties concerns stemming from ubiquitous surveillance of the motor-vehicle using population and poor confidence in retained data, would involve following the following principles. These principles are established under the assumption that there is a link between the license plate and personally identifiable information and that the following practices are needed in light of low data confidence.

**Practice One: Don’t store captured information**
Neither hit or non-hit data should be stored by the ANPR database systems. Instead, where there is probable cause to pull a vehicle and its occupants over for a traffic stop, relevant information should be kept in existing log books as legally required instead of uploaded to, and retained in, an ANPR database.

**Practice Two: Hit categories should be restrictive**
There should be probable cause to investigate a vehicle or the person operating it. The categories that establish a 'hit' should, therefore, be either linked to vehicle plates alone or only used when
pursuing serious crimes (e.g. an Amber Alert for a missing child, or a murder or manslaughter linked to a specific plate number). In effect, the surveillance of the general population must be proportionate to the degree of harm posed to the population/community. Hit categories should only be expanded or added to through an open and public democratic process.

**Practice Three: Redress**
When a vehicle is stopped on the basis of ANPR information the occupant should be informed of the ANPR system’s involvement and given an opportunity to correct the record as appropriate (e.g. perhaps the vehicle is still identified as ‘stolen’ in the ANPR database despite having been returned, or the plate linked to an unlicensed driver who has subsequently been licensed).

**Conclusion**
Some, such as David Brin, insist that “[n]o matter how many laws are passed, it will prove quite impossible to legislate away the new surveillance tools and databases. They are here to stay” (Brin, 1998: 8-9). He insists that procedural mechanisms - that empower citizens to understand the actions and data collection of governments - are essentially the sole means to equalize mass surveillance and data collection power asymmetries. We disagree with this dystopian framing of surveillance and privacy today.

Our article has outlined a novel state surveillance system that is accompanied by a host of associated databases. Efforts to limit transparency into the system while assuring citizens that ANPR is there for good government and public order have had marginal effects in limiting BC advocates’ message; despite the efforts of law enforcement and the RCMP, information about the system has emerged into the public eye, and an independent government body, the OIPC, is investigating authorities’ use of the technology. In the UK, efforts to obfuscate ANPR deployments, as was the case in Project Champion, also reveal the potential to resist mass vehicular surveillance. In essence, the experience of advocates in BC shows that it is possible the challenge and, ideally, ameliorate the state’s creation of novel surveillance-driven databases.

Successes depend on a combination of media savvy, advocacy tactics, solutions that are amenable to state institutions, and considerable amounts of good luck. Privacy advocates have repeatedly demonstrated a capacity to resist and mediate onerous state surveillance and recent resistance to ANPR in BC will, ideally, be seen as a similar ‘success story.’ Where Brin is arguably correct is that, absent external pressures from citizens and members of policy networks tied to state-developed or -relied upon databases, no changes will occur. An active and interested citizenry that is willing and able to place pressure on government is required to resist state surveillance. While true that the state and its agents may want to increase citizen surveillance there is no necessary technological or political logic guaranteeing that state surveillance must increase over time: in the face of undue political pressure and attention such surveillance can, and will, be turned back.
Works Cited


23


Royal Canadian Mounted Police, “E” Division Traffic Services (RCMP “E” Division). (Date unknown). “Automatic License Plate Recognition (ALPR) Program’s Terms and Conditions For Participation within a Policing Jurisdiction.”


Victoria Police Department (VicPD). (2010). Email correspondence about ALPR released under ATIP.


