BIG DATA
SURVEILLANCE

SURVEILLANCE STUDIES CENTRE

10110
11001 **BIG DATA**
01101 SURVEILLANCE

Queen's UNIVERSITY · University of St Andrews · UNIVERSITÉ LAVAL · University of Victoria · uOttawa

CRISP — CENTRE FOR RESEARCH INTO INFORMATION, SURVEILLANCE & PRIVACY · BC CLA BRITISH COLUMBIA CIVIL LIBERTIES ASSOCIATION · OFFICE OF THE INFORMATION & PRIVACY COMMISSIONER for British Columbia — Protecting privacy. Promoting transparency. · International Civil Liberties Monitoring Group · The Office of the Privacy Commissioner of Canada

BIG DATA SURVEILLANCE PROJECT TEAM

WWW.BIGDATASURVEILLANCE.ORG

Project Director
David Lyon, Queen's University

Co-Investigators
Kirstie Ball, University of St. Andrews, U.K.
Colin Bennett, University of Victoria
David Murakami Wood, Queen's University
Valerie Steeves, University of Ottawa
Stéphane Leman-Langlois, Laval University

Collaborators
Academic Collaborators
Mark Andrejevic, Pomona College, U.S.
Lisa Austin, University of Toronto
Andrew Clement, University of Toronto
Kevin Haggerty, University of Alberta
Alice Marwick, University of North Carolina, U.S.
Torin Monahan, University of North Carolina, U.S.
Carrie Sanders, Wilfrid Laurier University
Scott Thompson, University of Saskatchewan
William Webster, University of Stirling, U.K.

Partner Organization Collaborators
Michael McEvoy, Office of the Information and
 Privacy Commissioner for B.C.
Tim McSorley, International Civil Liberties
Monitoring Group
Christopher Prince, Office of the Privacy
Commissioner of Canada
Micheal Vonn, B.C. Civil Liberties Association

Partners
Civil Liberties
B.C. Civil Liberties Association (BCCLA),
Vancouver, B.C.
International Civil Liberties Monitoring Group (ICLMG),
Ottawa, Ont.

Privacy
Office of the Information and Privacy Commissioner
(OIPC BC), Victoria, B.C.
Office of the Privacy Commissioner of Canada (OPC),
Ottawa, Ont.

Academic
Centre for Research into Information, Surveillance and
Privacy (CRISP), University of Stirling, University of
Edinburgh, and University of St. Andrews, U.K.

Universities
Laval University, Que.
University of Ottawa, Ont.
University of Victoria, B.C.
University of St. Andrews, U.K.
University of Stirling, U.K.

Staff
Joan Sharpe, Project Administrator, Queen's University
Emily Smith, Research Associate, Queen's University

Post-doctoral Fellows
Ciara Bracken-Roche, University of Ottawa
Jeffrey Hughes, University of St. Andrews
sava saheli singh, Queen's University
Sachil Singh, University of Ottawa

Students
PhD
Jorge Campos, University of St. Andrews
Thomas Linder, Queen's University
Michael Carter, Queen's University
Debra Mackinnon, Queen's University
Brent Nellis, University of Ottawa
Smith Oduro-Marfo, University of Victoria
Midori Ogasawara, Queen's University
Jessica Percy Campbell, University of Victoria
Roger von Laufenberg, University of St. Andrews

MA
Jesse Gordon, University of Victoria
Roderick Hawes-Ospina, University of Ottawa
Robert Porter, University of Ottawa
Jenn Whitaker, Queen's University
Lauren Yawney, University of Victoria

LLB
Kathleen Selkirk, University of Ottawa

Research Assistants
Tim Charlebois, (MA student), University of Victoria
Eugenio Pazzini (MA student), University of Victoria
Didier Zuniga (PhD student), University of Victoria

Student Interns
Amelia Jarvis (MA student), University of Ottawa with
Valerie Steeves and ICLMG
Jesse Gordon (MA student), University of Victoria with
Colin Bennett and OIPCBC

CONTENTS

BIG DATA SURVEILLANCE:
AN INTRODUCTION

Funded through a Social Sciences and Humanities Research Council of Canada (SSHRC) Partnership Grant, the 'Big Data Surveillance' project (2015-2020) examines the relationship between big data and surveillance in three linked research streams: **security, marketing, and governance**. The project focuses mainly on the **vulnerabilities** generated by big data surveillance. In all three streams, the collection of big data and computation capacities tilt surveillance towards predicting outcomes and intervening to shape behaviours in advance. While big data is often celebrated as offering new advantages for surveillance, it also presents critical intellectual and policy opportunities for assessing the **social, political, and ethical issues** it presents.

In the world of big data surveillance, huge amounts of data are sucked into systems that store, combine, and analyze them, to create patterns and reveal trends that can be used for marketing, policing, and security. Big data and surveillance are neither "good" nor "bad," but they also are not neutral. Big data promises to further transform the ways that information and power are intertwined. Today, vast data-sets of personal information are assembled and analyzed in unprecedented ways and novel domains. They prompt fresh queries about **privacy, social sorting, and civil liberties**. Enthusiasm for big data techniques and practices has opened the door to mass surveillance as the main means of monitoring and tracking populations in order to manage and influence them.

Big data extends the scope of surveillance by co-opting individuals into participating in the surveillance of their own private lives. The ethical questions, political concerns, and moral challenges arising from the use of big data techniques protrude well beyond data protection and privacy rights. They penetrate the core of modern democratic principles. They are embedded, invisibly, in our everyday lives and in our decision-making.

Big data is a game-changer.

This SSHRC-funded project is led by Surveillance Studies Centre (SSC) Director David Lyon, with a team of five co-investigators, 13 collaborators, and five national and international academic and non-academic partners from civil liberties, privacy, and academic groups. The partnership project aims to reinforce our grasp of the issues, revamp policy initiatives, and reinvigorate public life today. Our objectives are to provide reliable baseline resources and solid research in each area, to show how big data affects change in these sectors, and to work with our partners to address emerging issues, both practically and ethically. Open the big data "black box" and we find a complex global collection of organizations (public and private), people (in commercial, governmental, academic, and global regulatory organizations), and practices (proprietary, legal systems and devices that initiate and sustain new data flows, their manipulation, and their use). Equally, terms such as surveillance and privacy have to be refined in light of big data.

> *"The goal of the Big Data Surveillance project is to understand the relationship between big data and surveillance in the three linked streams: 1. Security 2. Marketing and 3. Governance."*

"In the world of big data surveillance, huge amounts of data are sucked into systems that store, combine and analyze them, to create patterns and reveal trends that can be used for marketing, policing, and security."

APPROACH

Each research stream investigates:

· how big data analytics open up new forms of surveillance, or support existing trends, in their targeting and sorting practices;

· how big data contributes to laterally clustered surveillance, or reinforces powerful hierarchies, or both, in new ways, and which groups are especially vulnerable to these practices; and

· in what specific ways existing policy responses and instruments require radical overhaul and how far best practices may be developed to address emerging critical issues.

The goal of the Big Data Surveillance project is to understand the relationship between big data and surveillance in three linked streams: l. **Security** 2. **Marketing** and 3. **Governance**. Each stream involves personal datasets and the meshing of public and private sectors. This project examines both the internal dynamics of each stream and the practical connections among them, such as data-flows from one to another, in ways that affect practice.

STREAM ONE
SECURITY

STREAM LEADERS – David Lyon, Stéphane Leman-Langlois, and David Murakami Wood[†]

RESEARCH

This stream examines the scope and impact of big data-dependent "national security" surveillance of communications in the wake of Edward Snowden's 2013 revelations about National Security Agency surveillance. Both the National Security Agency (NSA), in the United States, and Canada's Communications Security Establishment (CSEC), intercept and store millions of emails and other messages. This is evidence of a shift to a big data approach. Documents and details disclosed to the media by Snowden indicate not only the scope but also the national and international range and complexity of big data practices, in which marketing and security surveillance operate in tandem. Our research examines this global trend, especially as seen in the programs, activities, and public documents of CSEC, the Canadian Security Intelligence Service (CSIS), and the Royal Canadian Mounted Police (RCMP). **What are the consequences of the shift from causation to correlation and for privacy and data protection regimes that are sidelined by this approach? How can surveillance be made transparent and public debate facilitated? What new policy directions are required?**

RESULTS

New research conducted in Stream One at the Surveillance Studies Centre focused on Canada's Signals Intelligence (SIGINT) organization and the Communications Security Establishment (CSE). We examined the physical infrastructure of CSE, especially the commissioning and building of its new headquarters in Ottawa, as well as the strategic priorities within the organization. Our initial research revealed the network of the public-private partnerships that built, and continue to operate, the CSE building with the same corporations that work with the NSA. This indicates close collaboration between, and similar methods in, each agency. We then conducted a study of the strategic direction of working practices inside CSE, based on Access to Information (ATI) requests on "big data" in CSE. This research has established definitively that an explicit transition to big data practices and quantitative analytics has been taking place in the CSE, which reflects a broader transition within security intelligence work.

This finding was presented, with other cutting-edge research on security intelligence, at a research workshop in Ottawa in October 2017. Topics included signals intelligence in Canada, resistance, regulatory challenges, security, policing, government, corporate, and technical challenges. In all, 21 papers were presented in eight sessions over two days to about 40 participants. From the work presented at the workshop, the need for greater transparency, accountability, and legal regulation and protection in security intelligence became clear. The **workshop results** are featured on our BDS website, which highlights key outcomes and related information in an accessible format. The workshop will also produce the **open-access book,** *Security Intelligence and Surveillance in the Big Data Age: The Canadian Case*, **edited by David Lyon and David Murakami Wood, UBC Press (forthcoming 2019).**

TRAINING AND MENTORING

The research projects completed in this stream have been largely due to the exceptional work of **Scott Thompson**, a post-doctoral fellow under the mentorship of David Lyon.

[†]From July 2015 to November 2017

KNOWLEDGE MOBILIZATION

A report by PhD candidates Steven Richardson and Debra Mackinnon outlines the adoption and engagement of wearable technologies in Canada and the implications for regulatory and privacy frameworks. It features an inventory of wearable technology in workplaces as well as best practices and recommendations. This report is the outcome of a one-year project under the 2016–2017 Contributions Program of the Office of the Privacy Commissioner of Canada.

Wearables in the Workplace
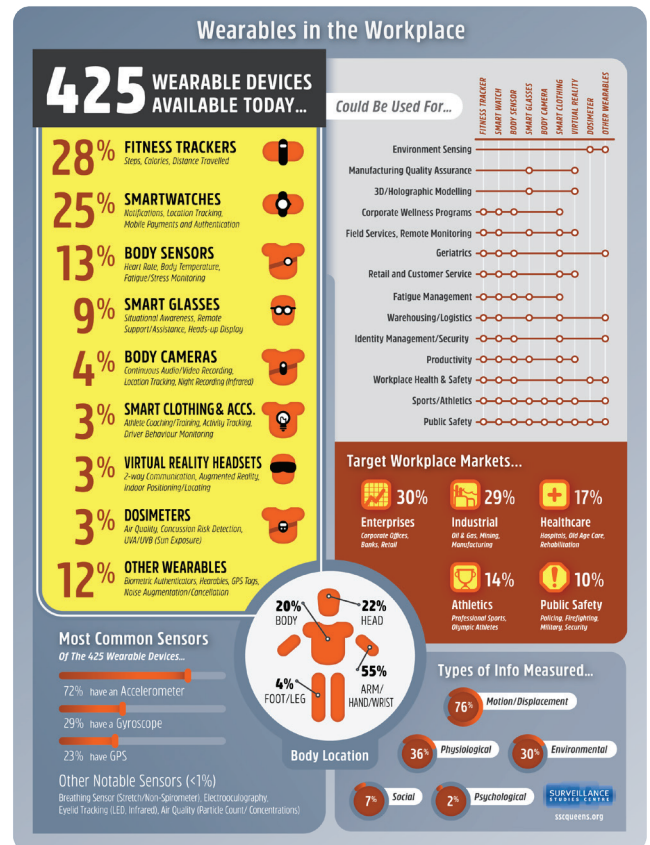
Dr. Thompson started a new tenure-track position at University of Saskatchewan in July 2017, but remains a collaborator in the partnership. The BDS partnership successfully recruited and funds **three PhD students** at Queen's: **Thomas Linder**, who played an important role in assisting with the Ottawa workshop organization as well as developing his own big data-related research agenda; **Midori Ogasawara**, who presented her work on national security agencies and related corporations at the October workshop; and **Debra Mackinnon**, who. with PhD candidate Steven Richardson, co-authored a report for one of our partner organizations (OPC) on wearable technologies. The research of other students also contributes to the work of Stream One. The Queen's node also hired **sava saheli singh** as a **post-doctoral fellow** beginning January 2018 to work on developing the free and publicly available online educational tool on Big Data Surveillance.

FUTURE DIRECTIONS

Stream One research/workshops have identified a new priority in this field: technology procurement for intelligence, policing, and data-gathering. Pending funding, we are planning a spin-off workshop on these important issues.

STREAM TWO
MARKETING

STREAM LEADERS – Kirstie Ball and Colin Bennett

RESEARCH
This stream examines how the massive data accumulation, analytical techniques, and associated applications have changed practices of marketing and political campaigning. We seek to find out how big data analytics used in the consumer world are now spreading into the political realm, shaping political campaign activity. Our research involves two case studies: consumer data donation and political campaigning.

"Consumer data donation" involves consumers parting voluntarily, even altruistically, with their consumption data in return for customized products and services. Data donation adds to the multiple data streams now analyzed by "big data" marketers, but promises to circumvent ethical problems around consent, purpose specification, and data limitation. The marketing stream studies whether big data practices that include data donation can be socially responsible.

Big data resources are also vital for **political and electoral analysis**. CRM, or customer relationship management, in the marketing world, has extended to VRM, or "voter relationship management". Citizens' personal data are collected and processed to influence their behaviours and decisions. The marketing stream delves into significant trends in this area, all facilitated by big data analytics:

- · the development of voter management databases,
- · the integration of personal data from commercial data brokerage firms,
- · the decentralization of data to local campaigns,
- · the targeted sharing through social media, and
- · the "micro-targeting" of increasingly refined segments of an electorate.

RESULTS
The marketing side of Stream Two uses the big data surveillance analytics "activity chain" as its unit of analysis and breaks this down into: project implementation, marketing practices, and consumer responses. A series of doctoral and post-doctoral projects examine the surveillant logics at play at each point in the chain. The research undertaken in the marketing side of Stream Two is informed by research completed under the SSHRC-funded Major Research Collaborative Initiative (MCRI), "The New Transparency," which exam-

SURVEILLANT/DATAVEILLANT
Logically, 'surveillant' means 'that which surveills' but this could be either a human watcher or a device like a phone or a system like social media. 'Dataveillant,' however, is much less common and refers primarily to the latter, that is, surveilling by data to monitor and track activity.

ined the intersection between big data and data protection. This research revealed that companies that used big data were driven by dataveillant objectives: they were keen to use analytics to manipulate the behaviour of customers.

This theme has been picked up by a number of parallel projects, which examine surveillance logics at different points in the big data activity chain. Three researchers have been recruited at the University of St. Andrews to complete these research activities. The first of two workshops, *New Lines of (In)sight: Big Data and the Analytically Driven Organization*, is being held at the University of Stirling, Scotland in June 2018, in partnership with the Centre for Research into Information, Surveillance and Privacy (CRISP).

Stream Two also analyzes the ways in which marketing logics and technologies have entered the political realm. It is now commonly asserted that modern election campaigns need to be "data driven". Our research undertaken examines the meaning of this phrase and the implications of using big data analytics in the electoral realm. It questions how they, and their surveillant logics, have influenced modern democratic elections and explores what the implications are for privacy, civil liberties and other democratic values. A second workshop on political micro-targeting and surveillance will be held in the fall of 2019, to coincide with the Canadian federal election.

TRAINING AND MENTORING
Numerous projects in this stream are being completed by **four doctoral students, two MA students, and one post-doctoral fellow**. Two of the doctoral students are in the University of St. Andrews doctoral program, with attendant opportunities through the Scottish ESRC Doctoral Training Centre, the Surveillance Studies Summer Seminar (Queen's), and the CRISP Biannual Doctoral Training School. The post-doctoral researcher, Jeffery Hughes, participates in the University of St. Andrews "Research Passport" training and development program. He also collaborates with Stream Two leader Colin Bennett on two papers related to political marketing and big data. University of Victoria doctoral students are given opportunities for social media engagement, co-publication, and attendance at conferences (including the Surveillance Studies Summer Seminar at Queen's).

KNOWLEDGE MOBILIZATION

PUBLICATIONS

Ball, K., DiDomenico, M. and Nunan, D. (2016) Big Data Surveillance and the Body – Subject. *Body and Society*, 22 (2), pp. 58 – 81.

Bennett, C. (2018) Cambridge Analytica shows the perils of voter analytics industry, *iPolitics*, https://ipolitics.ca/2018/03/21/cambridge-analytica-shows-the-perils-of-voter-analytics-industry/

Bennett, C. (2016) Voter databases, micro-targeting, and data protection law: can political parties campaign in Europe as they do in North America? *International Data Privacy Law*, 6 (4), pp. 261-275.

Bennett, C. with Bayley, R. M. (2015) Privacy Protection in the Era of 'Big Data': Regulatory Challenges and Social Assessments. In van der Sloot, B, Broeders, D. and Schrijvers, E. eds. *Exploring the Boundaries of Big Data*, Amsterdam: Amsterdam University Press, pp. 205-227.

Bennett, C. published a series of Op-Eds on voter surveillance in Canada in *iPolitics* during the last federal election: https://ipolitics.ca/author/colin-bennett/

STREAM THREE
GOVERNANCE

STREAM LEADERS – Valerie Steeves and David Murakami Wood

RESEARCH
This stream interrogates how big data analytics reshape prediction, pre-emption, and prevention in governance relationships. We study how citizens' lives are logged through mundane policy, such as smart meters. We also catalogue police information practices, to find out which privacy and fairness principles are being overwhelmed by big data practices. Strict limits on police powers to place citizens under surveillance go to the heart of democratic governance. Big data challenges these limits, in three interrelated ways:

1. Current regulatory frameworks draw sharp lines between private spaces (which are protected from warrantless access on the part of the state) and public spaces (which are not). However, this clear divide is blurred when police link location data from a variety of sources (cell phones, social media, video traces) with data continuously collected and shared by smart environments and surveillance drones.

2. Although police are not allowed to search a person or a home, without a warrant, data that emanate from those sources are increasingly collected by corporations and later voluntarily shared with police. Big data promises to increase exponentially this flow as sensors embedded in our bodies, homes, and electronic devices routinely collect information about our communications, interactions, physical health, and state of mind. The blurring of public and private spaces and data flow enable police to capture the intimate details of daily life, thus changing their relationship with citizens.

3. Big data logic may overwhelm the legal mechanisms we rely upon to ensure that the police cannot overreach their authority and upset the democratic balance of power between state and citizen. The law assumes that judicial oversight limits police use of surveillance limiting it to the stated investigation, and to a specific place and/or period of time. Big data analytics, however, work very differently, pre-emptively collecting all data, however mundane, on an ongoing basis and analyzing it for unknown patterns. Police use of big data threatens to reverse the presumption of innocence because the algorithm treats all citizens as potential criminals who must be monitored and controlled.

RESULTS
This stream has conducted an analysis of the judicial approaches to emerging police uses of big data, with special emphasis on cell tower data dumps and International Mobile Subscriber Identity (IMSI)-catchers. Qualitative interviews were undertaken with key informant civil society advocates and hacktivists, to deepen our understanding of the emergence of the anti-surveillance movement as a response to the expansion of police powers in Bill C-51. We are also investigating the big data facility opened in 2017 by the Ottawa Police Force, the use in Ontario of data hubs that share information

We ask: How does law enforcement in Canada use big data for investigative and preventive purposes? How far is this a "new surveillance"? How should privacy and fairness be secured in this circumstance? How do emerging big data technologies affect the experience of citizenship for crime suspects and ordinary citizens?

between police, social services, and non-governmental agencies to preemptively identify potential criminals to prevent crime, and the interaction between police and smart citizen initiatives in Toronto and Vancouver. The latter two sub-projects highlight how big data logics have migrated from policing to other governance contexts; we are now including education, health, and religious institutions.

TRAINING AND MENTORING

Stream Three has **two MA students, one LLB student, one doctoral student**, and **two post-doctoral researchers** at the University of Ottawa. Post-doctoral researcher Sachil Singh, along with Valerie Steeves are in the process of obtaining ethics approval to conduct follow-up interviews with practitioners to explore practices in the Point of Care tools used in Ontario hospitals. The first BDS-initiated **partner/student internship** has also now begun. Valerie Steeves supervises an MA student who spends one day per week working at the ICLMG on a dedicated project related both to her MA work and a priority area of background research for ICLMG.

FUTURE DIRECTIONS

This stream has expanded to encompass governance models emerging in a variety of institutional arenas that rely on big data to provide care of – or control over – persons. Our focus includes education, health-care, and religious institutions. This has been highly effective, enabling the stream to examine how big data analytics are (re)shaping governance within a broad range of social contexts. A research workshop is planned for the final year of the project, 2020, on "A Deliberative Dialogue with Citizens: Regulating Big Data Surveillance".

KNOWLEDGE MOBILIZATION

Valerie Steeves developed a day-long workshop for teachers, school administrators, and privacy policymakers exploring emerging issues, including "personalized" educational software that uses big data algorithms and algorithmic surveillance of students on social media. The workshop was delivered in the fall of 2017 in Alberta, in partnership with the Alberta Information and Privacy Commissioner and the Alberta Teachers' Association, and in Ontario, in partnership with the Ontario Information and Privacy Commissioner.

BIG DATA 175

BD175 (Big Data Event Series) within the Queen's University 175th anniversary celebrations 2016-2017. See: http://www.sscqueens.org/projects/big-data-surveillance/bd175

This series of events at Queen's University raised the profile of big data activities on campus and invited discussion among faculties, schools, and departments. Several events showcased our research on Big Data Surveillance, and involved team members from both Queen's and our partners. The events were accessible to students, faculty, staff, and the wider Kingston community, engaging them in these pressing public issues and showcasing the multidisciplinary leadership of the academic community on big data. Through a multi-media approach, including panel discussions and lectures, film screenings and art exhibits, the **3-Ds** of big data were addressed. They:

- **Defined** the genesis and character of big data, where it came from and what it is;
- **Described** how big data is used in various contexts and its common features; and
- **Debated** the ethical questions of how and if we should use big data.

This series offered monthly events from the fall of 2016 into the winter of 2017.

SURVEILLANCE STUDIES SUMMER SEMINAR

Surveillance Studies Summer Seminar (SSSS), Theme: Surveillance in the Big Data Era, Queen's University, June 15–21, 2017. See www.sscqueens.org/projects/surveillance-studies-summer-seminar

The biennial Surveillance Studies Summer Seminar was held in June 2017; its theme was "Big Data Surveillance". Twenty top PhD students from Canada, the U.S., Europe, and the Middle East took part in this highly successful intensive doctoral school led by Torin Monahan (University of North Carolina at Chapel Hill), David Murakami Wood (Queen's University), and Scott Thompson (Queen's University). Participants learned directly from top researchers in the field of surveillance studies, as well as technical experts, through a series of seminars. The presentation of papers, plus the professional development and networking components of the program, provided tangible benefits to their own research projects. The full line-up of invited speakers for 2017 included: Don Aldridge (Queen's University High Powered Computing Centre, and formerly with IBM), David Lyon (Queen's University), Stefania Milan (Amsterdam), Mark Salter (University of Ottawa), Kristin Veel (Copenhagen), and Jennifer Whitson (University of Waterloo).

Next Surveillance Studies Summer Seminar (SSSS), Queen's University, June 2019

1- SSSS group photo from 4S17 in front of the Isabel Bader Centre at Queen's University, June 2017
2- BDS 175 logo
3- Frank Pasquale and Evelyn Ruppert discuss big data futures at the panel discussion concluding the BDS175 events in March 2017 at Queen's University

OUTREACH EVENTS

RESEARCH IN ACTION

ATIP REPOSITORY

Access to Information (ATIP) and Freedom of Information (FOI) research methods are part of the BDS methodological approach. These released documents detail the workings of government departments and agencies, providing key insights into how surveillance and big data are working within our society. With the project's acquisition of thousands of pages of relevant documents, it became important to share these sources within the larger academic community and with the general public. The inclusion of these documents became the project's overall knowledge mobilization goals.

As a result, **an online repository for all Canadian Access to Information (ATIP) and Freedom of Information (FOI) requests** regarding surveillance programs is being made available by the SSC in partnership with the Queen's University Library. **The first of its kind in Canada**, this tool makes the full texts of all released documents available and searchable to other researchers, students, the press, and the general public. In this way, the Surveillance ATIP/FOI Repository acts not only as a means of disseminating knowledge, but also works to fulfill SSHRC's requirement of making research data available to the general public. By giving researchers and others direct access to previously released ATIP and FOI requests, this new repository opens up these datasets to be used as educational tools in the classroom, eliminating ATIP/FOI wait times and costs. This all benefits teaching and student research opportunities, both at the undergraduate and graduate levels. Scott Thompson, previously a post-doctoral fellow on the project and now a collaborator, worked in conjunction with staff at Queen's University Library to develop the technological infrastructure of the repository and ensure user accessibility and functionality. The system will be publicly launched in 2018.

EDUCATIONAL MEDIA:

Privacy in the age of big data

Surveillance affects all Canadians, but few citizens are aware of how, when, for what purpose, or with what consequences their personal data are used by large organizations. The Surveillance Studies Centre (SSC) and the BDS (Big Data Surveillance) project, partly funded by the Office of the Privacy Commissioner's Contributions Program, is producing three short films and complementary educational resources ranging from supporting curricula, to infographics and animated gifs that will address issues around surveillance technologies and privacy, including the economics of personal information, government surveillance, reputation and privacy, and the body as information. The video vignettes will cover:

1. **Privacy and social media: online surveillance**
2. **Privacy and movement: smart cities as big data surveillance**
3. **Privacy and the body: wearables and big data**

This project is led by BDS Post-doctoral fellow sava saheli singh. The goal of this knowledge translation project is to reach a broad audience and increase public understanding on issues of widespread surveillance systems and technologies, and on controlling and enhancing data privacy practices. Importantly, **emphasis will be placed on the social consequences of surveillance for institutions and ordinary people, with ethics, privacy, civil liberties, and human rights at the fore.**

EXTENDING PARTNERSHIPS/ NEW RESEARCH DIRECTIONS

Our partners both help to guide the research and make vital use of its findings in developing new policy and practices. Partners have expertise in assessing surveillance practices and have connections with data practitioners in security, marketing, and governance. We identify common issues with the use of big data in relation to vulnerable populations. Our academic partner, the Centre for Research on Information, Surveillance and Privacy (CRISP) follows similar situations of big data development and of globalized civil society responses. Our policy-and-advocacy partners, the BC Office of the Information Privacy Commissioner (OIPCBC), the B.C. Civil Liberties Association (BCCLA), the federal Office of the Privacy Commissioner (OPC), and the International Civil Liberties Monitoring Group (ICLMG), are involved in contextualizing and explaining major long-term trends in surveillance and using the research to gain greater understanding of the role of big data surveillance, as well as developing new policy practices based on the findings. We aim to work together to advance knowledge of current developments in surveillance and regulation that will, in turn, promote privacy, civil liberties, and human rights. Together, we seek cutting-edge knowledge of developments in surveillance, big data, best practices and regulation, for the common good.
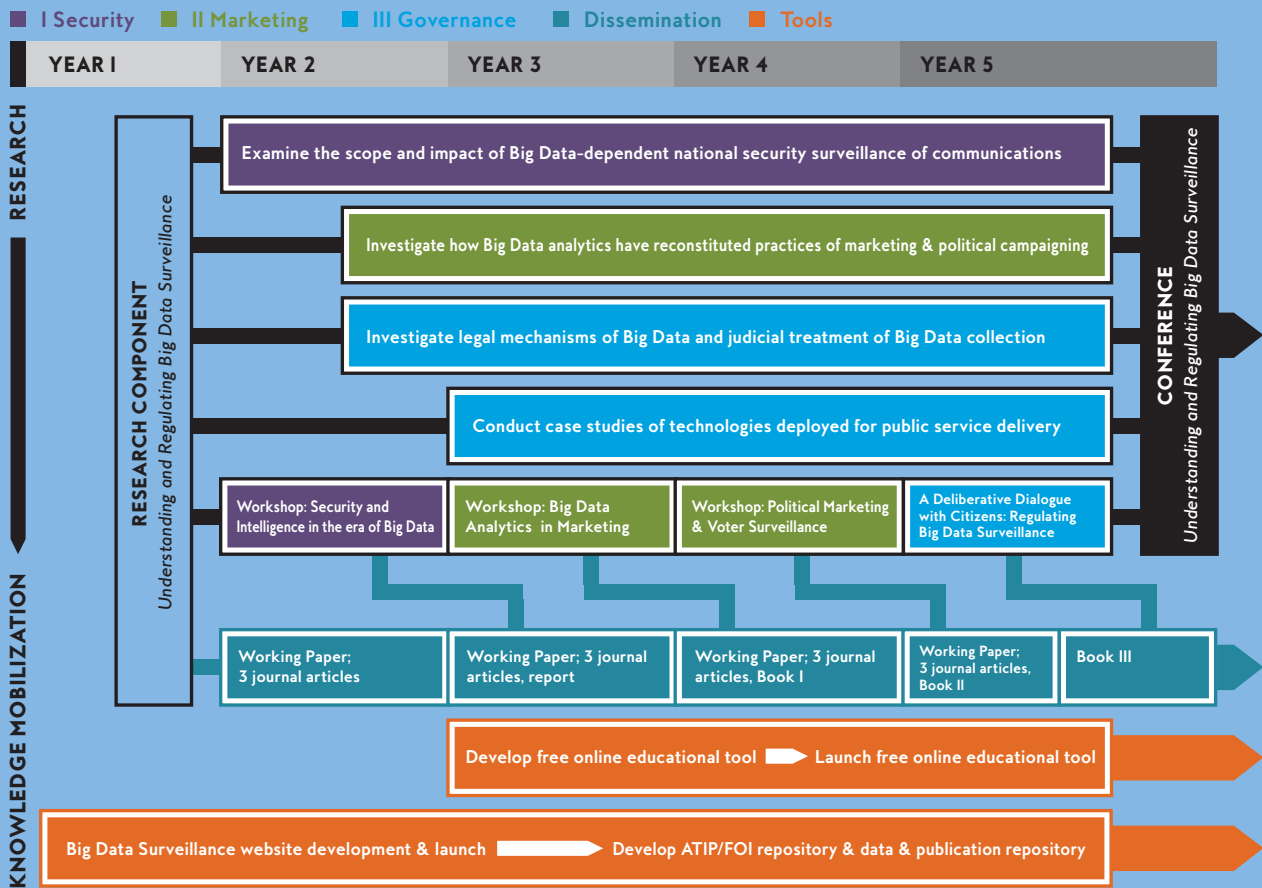
SIDEWALK LABS RESEARCH

In March 2018, we held a research meeting in Toronto, prompted by the announcement of the "Sidewalk Labs" project from Alphabet/Google, who plan to rejuvenate part of the old dockland area in Toronto with a new concept of urban design, "from the internet up". Consistent with Google's business plan, this means using big data to track and monitor all systems and populations, "smart city" style. David Lyon and David Murakami Wood, who proposed the meeting, met with others from privacy and civil liberties groups, as well as BDS collaborator Andrew Clement and PhD students Debra MacKinnon and Michael Carter. Several group members have accepted invitations to be on advisory panels. Another meeting is planned for the fall of 2018. This project falls under BDS Stream Three.

VOTER SURVEILLANCE AND CAMBRIDGE ANALYTICA

News broke in March 2018 that Cambridge Analytica had used the data from 87 million Facebook users to target potential Trump voters in the Presidential election in 2016, thus highlighting an issue already signalled for attention in the BDS research program. As with Sidewalk Labs, the issues are profoundly surveillant, raising basic issues of democratic participation as well as the privacy of personal information. Colin Bennett has published opinion pieces on the topic, for instance in *iPolitics*, while David Lyon and others discussed it in the media. A student intern has been hired for the summer to work with OIPCBC on data analytics and Canadian elections. This is a major theme of a Stream Two research workshop planned for 2019 in Victoria, B.C.

FUTURE EVENTS

Appendix I – 4.0 Organization of Activities

I Security **II Marketing** **III Governance** **Dissemination** **Tools**

YEAR 1	YEAR 2	YEAR 3	YEAR 4	YEAR 5

RESEARCH

KNOWLEDGE MOBILIZATION

RESEARCH COMPONENT
Understanding and Regulating Big Data Surveillance

Examine the scope and impact of Big Data-dependent national security surveillance of communications

Investigate how Big Data analytics have reconstituted practices of marketing & political campaigning

Investigate legal mechanisms of Big Data and judicial treatment of Big Data collection

Conduct case studies of technologies deployed for public service delivery

CONFERENCE
Understanding and Regulating Big Data Surveillance

Workshop: Security and Intelligence in the era of Big Data

Workshop: Big Data Analytics in Marketing

Workshop: Political Marketing & Voter Surveillance

A Deliberative Dialogue with Citizens: Regulating Big Data Surveillance

Working Paper; 3 journal articles

Working Paper; 3 journal articles, report

Working Paper; 3 journal articles, Book I

Working Paper; 3 journal articles, Book II

Book III

Develop free online educational tool ➔ Launch free online educational tool

Big Data Surveillance website development & launch ➔ Develop ATIP/FOI repository & data & publication repository

FUTURE WORKSHOPS

INAUGURAL RESEARCH WORKSHOP	STREAM-LED INTEGRATED RESEARCH WORKSHOPS				FINAL CONFERENCE
	STREAM 1: SECURITY	STREAM 2: MARKETING	STREAM 3: GOVERNANCE		
MAY 12-14 | 2016	OCT 19-20 | 2017	JUNE 4-5 | 2018	2019	2020	2020
WORKSHOP	WORKSHOP	WORKSHOP	WORKSHOP	A DELIBERATIVE DIALOGUE WITH CITIZENS	CONFERENCE
QUEEN'S UNIVERSITY	UNIVERSITY OF OTTAWA	UNIVERSITY OF STIRLING, U.K.	UNIVERSITY OF VICTORIA		QUEEN'S UNIVERSITY
KEY ISSUES IN BIG DATA SURVEILLANCE	SECURITY INTELLIGENCE AND SURVEILLANCE IN THE BIG DATA AGE	NEW LINES OF (IN)SIGHT? BIG DATA SURVEILLANCE AND THE ANALYTICALLY DRIVEN ORGANIZATION	POLITICAL MARKETING AND VOTER SURVEILLANCE	REGULATING BIG DATA SURVEILLANCE	UNDERSTANDING AND REGULATING BIG DATA SURVEILLANCE
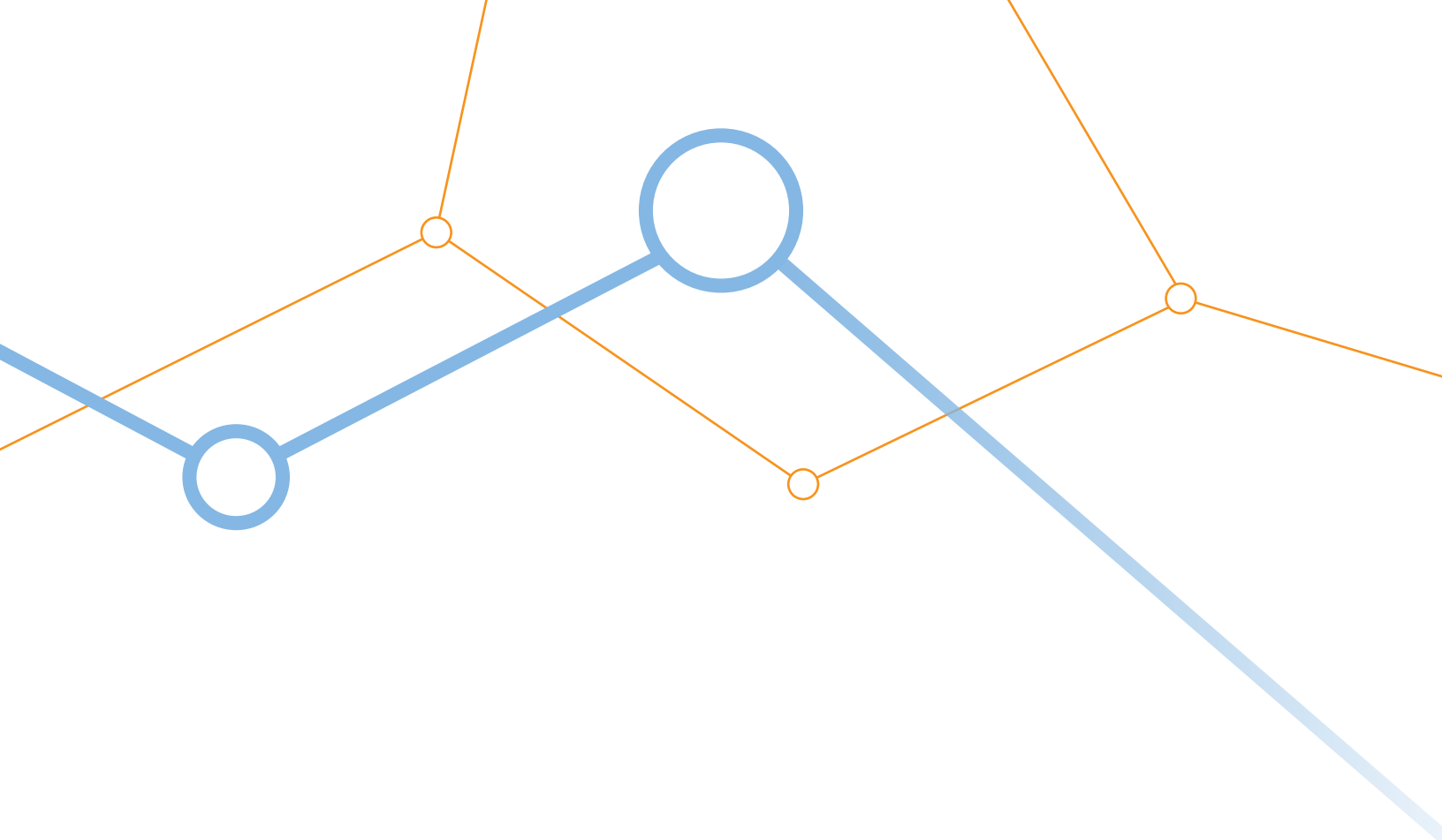
The Surveillance Studies Centre (SSC) at Queen's University is committed to high-quality research on the growth of surveillance globally, exploring many aspects of contemporary monitoring, tracking, management, and control. The SSC is part of a broad network of surveillance research that is both multi-disciplinary and international.

www.sscqueens.org
Twitter: @sscqueens
surveill@queensu.ca

Our mailing address is:

Surveillance Studies Centre
c/o Department of Sociology
Queen's University
Kingston, Ontario K7L 3N6
Canada