ISSN 2042-5686 (Print)

iS CHANNEL

Volume 15
Issue 1

September 2020

Cover Image
From Remi Botbol.
Macro image of a silicon wafer. Each square is an individual chip with microscopic transistors and circuits. The silicon wafers are sculpted using photolithography and are then diced into their individual chips that make our modern microprocessors.

Formatting
Yue (Emma) Feng

Lay-Out Design
Yue (Emma) Feng

iSCHANNEL is available in PDF at http://lse.ac.uk/ischannel
Follow us on Twitter @ischannel

Contact
Information Systems and Innovation Group
Department of Management
London School of Economics and Political Science
Houghton Street
London WC2A 2AE
Email: is.channel@lse.ac.uk

Contents Page

Editorial
From the Faculty Editor
Will Venters 2

From the Associate Editor
Barbara Nitschke 3

Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees
Amy Vatcha 4

Addressing the Challenges Facing Decentralized Identity Systems
Andrei Volkov 10

Big Data in Smart Cities: A Critical Literature Review
Lisa Schaefer 16

Social Media Personalization Algorithms and the Emergence of Filter Bubbles
Sanveer (Sunny) Rehani 20

Social Media as a Data Source in the Public Sector: Socio-Technical Challenges for Economic Indicators
Keisuke Idemitsu 25

How Big Data Impacts Research and Knowledge Generation: An Epistemological View
Yiduo Wang 29

Perspectives on Business and Technology Alignmen
Jiao (Joanna) Peng 33

ICT Occasions Changes in E-Government: The Case of Elster
Christian Poeschl 38

EDITORIAL – From the Faculty Editor

This year has been dominated by the COVID and the changes it has wrought on the LSE. Yet the editorial team has produced the journal without help and with exceptional professionalism. For this they must be hugely congratulated. They now join the incredible multitude of iSChannel alumni from these past 15 years who have benefited so much for this journal!

This year I wanted to talk a little about reviewing for the iSChannel. Reviewers are, in some ways, the unsung heroes of any journal. While it might feel like a burden, reviewing is a wonderful chance to be forced to critically examine someone's writing and to make a recommendation. For MISDI and PhD students it gives a chance to experience what an examiner experiences judging their own work, and to learn the pitfalls we all make in our writing.

It is not the reviewers job to "decide" whether an article is "good"(accept) or "bad"(reject) – they can only make recommendations. Editors always decide. They act as peer-reviewers to the writer, examining and assessing, as equals, the argument and seeking to provide supportive advice which can develop the work. Reviewers engage with improving articles more than judging them – and in many ways they become co-authors of the articles they review. The following list provides a checklist for iSChannel reviews which may be helpful in the future.

- Provide a brief summary of the article – what kind of article is it? What issue does it seek to address?
- Discuss the overall validity of the argument made – does it hold together well? Is it convincing?
- Provide a polite overall judgement briefly setting out strengths and weaknesses as you see them. Acknowledge where you are unsure and that you only recommend editors make a decision. Write "I think" rather than "it is". Make your recommendation (Reject, Major Revision, Minor-Revisions, Accept-as-is).
- Carefully discuss each section of the article and provide suggestions for improvements for each part.
- End with a positive comment about the work.
- List minor points or correction which you noted (e.g. spelling errors, referencing errors…) but which should not affect your recommendation.

Reviews must be polite and never rude. Writers have worked hard on their articles and submitted their best work. It is disheartening to receive rejection but it is made worse when the reviews do not politely and clearly explain the failings or make any suggestions for improvement. Reviewers must also act ethically – if a reviewer feels in any way biased towards an article they should speak with the editor.

Reviewers should be proud of their important role. They can put reviewing on their CVs. Editors should also provide reviewers with feedback on their reviews (one sentence or so) that can be used on the CV. I therefore would like to particularly thank those who reviewed this year: Martin Lamby, Miriam Trocha, Nicola Ringele, Patrick Kohler-Aranibar, Yiduo Wang

I want to end with a word of thanks. This year's editorial team – Barbara Nitschke, Christian Poeschl, Keisuke Idemitsu, Konstantin Mangels, Maximilian Goehmann, Yue (Emma) Feng have been amazing and worked exceptionally well to deliver this journal. I would also particularly like to thank Jiao (Joanna) Peng who, as senior editor, has been instrumental in professionally delivering the iSChannel's 15th anniversary edition despite the challenges and in leading the team. Together the whole team delivered it earlier than usual to allow a longer printing and delivery time. Well done!

I very much look forward to the next 15 years of this amazing journal.

Will Venters

Faculty Editor

EDITORIAL – From the Associate Editor

In its 15th year of publication, the iSChannel again focuses on social aspects of information systems. The contributions therefore take neither technologically deterministic perspectives nor purely socially constructive viewpoints, but instead provide socio-technical analyses. This year we have again received a large number of submissions and are delighted to publish seven excellent papers.

Two articles focus on data privacy. In her highly topical article, **Amy Vatcha** examines contemporary forms of digital employee surveillance which in Corona times and massively increased remote work have gained high importance. **Andrei Volkov** discusses decentralised identifier systems as a new technical possibility for individual data control. However, they have to be modified to overcome the two key challenges of scalability and interoperability.

Three further articles concentrate on big data. In her critical literature review, **Lisa Schaefer** analyses big data in smart cities from a bounded technical-rational and a socially embedded viewpoint. The benefit of increasing cities' efficiency must be balanced with inherent privacy issues. **Sanveer (Sunny) Rehani** analyses how the technical infrastructure of social media platforms advances filter bubbles. Especially personalisation algorithms favour filter bubbles and thereby amplify opinion polarisation. **Keisuke Idemitsu** examines socio-technical problems of mining social media data to create economic prediction indicators. The author substantiates his analysis on the example of the Japanese government using Twitter and blog data to predict industrial production.

The three remaining articles centre around socio-technical consequences of datafication developments. **Yiduo Wang** describes in her critical literature review how the abundance of automatically collected big data has triggered an epistemic change within research theory generation. **Jiao (Joanna) Peng** summarises two opposing theories on business-technology alignment, namely rationally planned and improvised alignments. **Christian Poeschl** analyses how the adoption of a new technology transforms decision-making processes in the public sector. Based on the novel digital German tax declaration system Elster, he finds that decision speed and discretionary power are changed and a more formalised as well as homogeneous decision-making process emerged.

We would like to thank all authors and reviewers for their outstanding contributions for this year's 15th anniversary edition. Additionally, we would like to thank Will Venters, our faculty editor and the previous long-term senior editor, Marta Stelmaszak for their support in creating this issue. Covid-19 has considerably changed our studies at LSE and digitised our student community and campus life. It did not prevent us from jointly creating this issue, though, which we hope will find curious and kind readers.

Barbara Nitschke

Associate Editor

iS
CHANNEL

Workplace Surveillance Outside the Workplace: An Analysis of E-Monitoring Remote Employees

Amy Vatcha

MSc Management of Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Workplace Surveillance
E-Monitoring
Remote Employees
Privacy
Security

ABSTRACT

In the time of Covid-19, working from home has suddenly become the norm. This thematic literature review explores the workplace surveillance landscape for remote workers from an employee perspective. The literature considered includes information systems journals, management journals, regulation whitepapers, and technological solutions. This paper discusses the excessive surveillance that occurs, the technologies that facilitate it, why it erodes trust with employers, and what tools and frameworks employees can use to demand privacy. Employee surveillance is no longer confined to the office space, it is holistic, constant, round the clock monitoring, enabled by new technologies and lowering costs of existing technologies. I argue that remote employee acceptance of workplace monitoring solutions depends on the transparency on data collection from employers, and the exclusive use of the data for security rather than hiring and firing decisions.

I. Introduction

The presence of workplace surveillance is not a surprise to employees in white collar roles. In the context of remote working, the dynamic is unique because there are no physical boundaries between work and leisure hours. In this essay, I explore the specific context of remote working from an employee perspective, where the living room doubles as an office. Some employers offer flexible working accommodations such as working from home, or working from anywhere including co-working spaces such as WeWork, or an island in the Mediterranean. There are blurred boundaries between the home and office, which is problematic because employee surveillance extends beyond in-office monitoring to 24/7 surveillance. The surveillance technology is "unblinking" and "ever-present" (Nord, 2006). Employee surveillance is no longer confined to the office space, it is holistic, constant, round the clock monitoring, enabled by new technologies and lowering costs of existing technologies. The flexibility comes at a price, being the boss of one's own schedule literally means that one's boss can monitor employees anytime. The goal of employers offering flexibility is to improve employee-employer relationships, so excess surveillance would undermine these efforts.

Rather than broadly defining the concept of privacy, in the context of this paper it would be more appropriate to define the importance of privacy as "privacy thus possesses intrinsic value: it is essential for thinking and acting freely" (Stone-Romero and Stone, 2007). The Computer Security Institute (CSI) found that over 75% of companies faced issues with employees using illegitimate software, online shopping during work, accessing pornographic material, using work hours for childcare or napping, and using their work emails inappropriately (Nord, 2006; Bloomberg, 2020). To detect employees who are shirking their responsibilities during work hours, surveillance technology is employed. There is large scale systematic monitoring using software such as Spectorsoft, DynaComm, Investigator 2.0, and Silent Watch (Introna, 2002; Nord, 2006; Nockleby, 2002). These software solutions solve "an old puzzle made more complex with new software" (Nord, 2006). Investigator 2.0 is available for under $100 and sends summaries of all activities on a given PC, while Silent Watch even provides the exact typing patterns, so the technologies are already available at a lower cost than ever before (Nockleby, 2002). The root of the problem is the use of intrusive technologies without consent in private places such as the home of a remote worker. I argue that in the era of technology, flexible working, and fluid boundaries between the home and office, workplace monitoring for business reasons often extends into one's personal life leading to all round employee monitoring. Remote employee acceptance of workplace monitoring solutions depends on these factors - transparency on data collection from employers, clarification of data usage for system security or for hiring and firing decisions, and the avenues available for employee privacy concerns to be heard.

II. Why Excess Employee Surveillance Erodes Trust

What forms of surveillance are used? Which are considered "excessive"?

Corresponding Author
Email Address: vatcha.amy@berkeley.edu

Employers justify carrying out surveillance to protect company secrets and sensitive confidential information, protect themselves in case of liability issues such as discrimination or harassment, prevent 'time theft' where employees lie about their hours, discourage employees from carrying out non work-related tasks at work, or 'careless communication' which can expose the company's systems to phishing (Smith and Tabak, 2009). In an organization, there are various threats to data privacy such as phishing attacks, system security vulnerabilities, hackers gaining unauthorized access to the network, but employees are known to be the weakest link in organizational data privacy (Pigni et al., 2018; Culnan et al., 2009). For example, in the Target data breach in 2013, the initial access to the system was granted by an unsuspecting employee, the aftermath of which cost the company upwards of $18 million and a lifetime of irreparable public relations damage (Pigni et al., 2018). Moreover, today's labor market is evolving for the gig economy, with new employee categories such as independent contractors and outsourcing becoming increasingly common. Contractors are not bound by the same non-disclosure agreements as full-time employees are, which adds another layer of vulnerability to data privacy initiatives. Besides cybersecurity concerns stemming from employee negligence, employees can also tarnish the reputation of their employer if they engage with inappropriate social media posts even when they are not at work (Hyman, 2017). Social media posts are monitored because personal views of an employee can be tied to the company's public image. The public connotation of the data on the platform merges with the private aspect that is usually hidden from coworkers. Employers utilize workplace surveillance to monitor employee honesty while using it as a tool to prevent employees from engaging in unproductive and illegal acts at work including extra breaks, and safety shortcuts (Stone-Romero and Stone, 2007). The monitoring techniques include using contemporary technologies such as artificial intelligence, advanced analytics, mobility data, keystroke logging software, and social media, but the monitoring is considered excessive because it occurs round the clock including in an employee's personal time.

Why is employee trust necessary for employers?

Employee buy-in is necessary with any investment in workplace technology because employees would react negatively if their freedom is threatened or if the privacy invasion is unfair (Horton, 2020; Parks et al., 2017). According to an executive at Simply Communicate workplace consultancy, "tracking technology without clear well-communicated mutual benefit for both business and employee always struggles to get adoption or, worse, may be inadvertently or deliberately sabotaged by employees" (Horton, 2020). The necessity of employee surveillance has been compared to using security cameras at a bank, "not because of lack of trust...it's because it's imprudent not to do it" (Bloomberg, 2020). If employees comply with all of their duties, and companies are transparent with how they are tracking their employees, the hostility and pushback against surreptitious surveillance can give way to a solid trust relationship. As a Bloomberg article for managers suggested, "if you hired them, you should trust them" (Bloomberg, 2020). Value-driven companies aim to protect the interests of their stakeholders, and employee monitoring is inconsistent with this message to the company's most valuable asset: their staff.

Why does excess surveillance erode trust?

The power dynamic between employers and employees is incredibly asymmetrical. Employers are in a position of power through the contracts that employees sign, the paychecks they are in charge of, and the terms and conditions of being on the job. Employees can be constantly monitored, i.e. "passive surveillance", rather than actively surveilled where particular employee's actions have sparked the suspicions of the system (TUC, 2017). Passive surveillance is the prevalent form of employee monitoring today, involving 'blanket' monitoring of all employees regardless of individual justification (TUC, 2017). Active surveillance focuses on depth rather than breadth of surveillance, with particular individuals being closely monitored (TUC, 2017). Active surveillance is problematic because it is more susceptible to human bias. Executives have access to more confidential information and information systems than junior employees do. Yet, active surveillance mechanisms scrutinize junior entry-level employees at a higher rate than executives are monitored (TUC, 2017). An e-monitoring solution called Hubstaff conducts dynamic surveillance according to job title (Bloomberg, 2020). Companies need to calculate if the loss of employee morale created due to surveillance is worth the value that surveillance brings (Horton, 2020). If employers trusted their employees, they would measure their performance output instead of effort input (TUC, 2017). E-monitoring erodes psychological trust where the perceived risks of the monitoring system cannot be controlled by the employee so they lack control over their personal information (Ozdemir et al., 2017).

III. Why Employee Monitoring is Holistically Intrusive

Surveillance starts before an employee is even onboarded! The background check is the starting point for workplace surveillance, before a candidate has even signed their employment contract. Background checks previously provided a one-time snapshot of past crimes, but now in the USA, the FBI's RAP BACK program allows employers to receive continuous information about their employees and their involvement with petty crime or police (Kofman, 2017). New technologies enable new kinds of holistic surveillance techniques, but also bring down the cost of monitoring. For example, the FBI's RAP BACK program only costs an employer $13/person monitored (Kofman, 2017). Opt-in or opt-out is not feasible because this kind of surveillance is mandatory in employment contracts (D'Acquisto et al., 2015). Candidates in the pipeline also have their social media accounts parsed.

Employee monitoring is holistically intrusive because it extends beyond the boundaries of work-

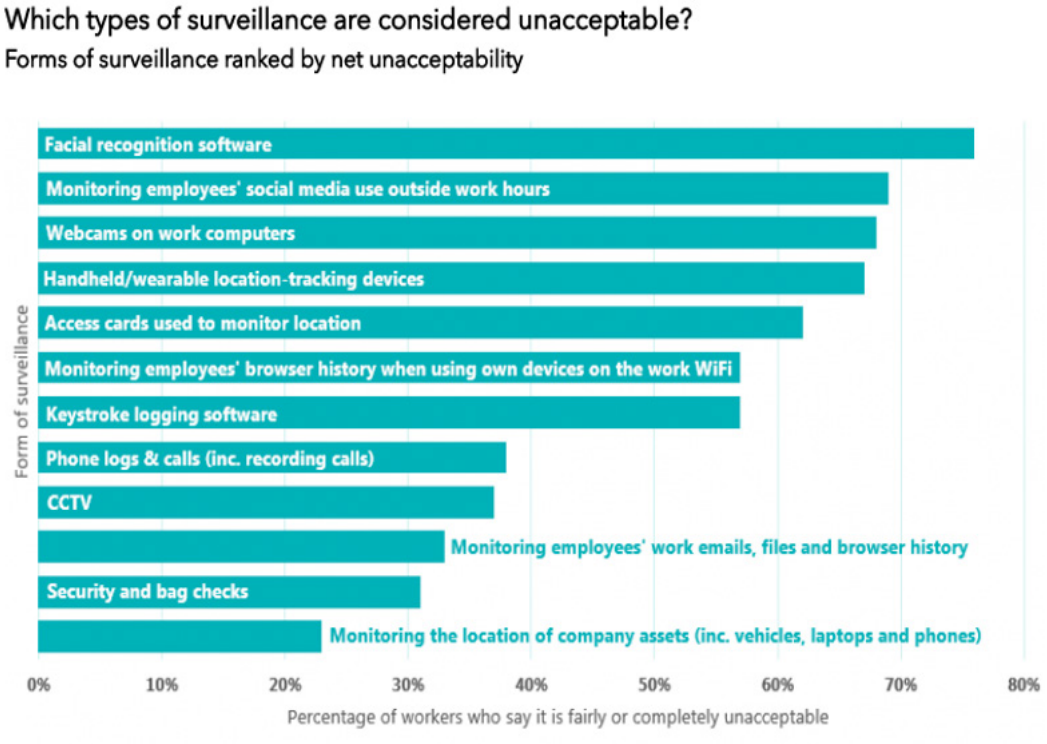
related surveillance. In the case of remote working, the forms of surveillance include computer log on and off times, location tracking of work phones and laptops, search history typing speed, keystrokes (including passwords), call logs, instant messenger chat response speed, and emails scanned for financial crime such as insider trading (Jeske et al., 2015; TUC, 2017; Bloomberg, 2020). Arguably, tracking computer logon and logoff times is parallel to in-office workers who are tracked by how much time they spend at work via badge scans (Horton, 2020). Barclays uses heat sensors and motion detection to track employee presence, but claims that this information is collected to optimize office space and floor layout (Horton, 2020). Office desktop monitoring is not a new phenomenon, but it "seems a violation of privacy to a lot of workers when they're required to have software on their computers that tracks their every move in their own homes'' (Bloomberg, 2020). According to Gartner, employee monitoring will occur in 80% of companies by 2021 (Horton, 2020). Covid-19 has made e-monitoring software solutions popular such as InterGuard, Time Doctor, Teramind, VeriClock, innerActive, ActivTrak, and Hubstaff (Bloomberg, 2020). A software called Sneek takes pictures of an employee every five minutes via webcam to check if they are at work, and companies have access to a "wall of faces'' to monitor them at a glance (Holmes, 2020). These technological solutions can be used outside of standard working hours (Horton, 2020). The judgements from after-hour monitoring can leak into workplace compensation decisions (TUC, 2017). The chart below ranks the forms of surveillance according to employee unacceptability (TUC, 2017).

Lack of Transparency around Data Collection Methods

Remote employees can be monitored by their internet use, social media posts, audio from their work laptops, phone calls, mobility data from their work phone, every email that flows through their work email account, every file saved on a work computer, and every keystroke typed (Ball, 2010; Bowcott and Rawlinson, 2017). If an employee turns off their company issued mobile phone to disconnect from work on the weekend, their offline status can be detected. New technologies are enabling e-surveillance and employers are "harnessing the emergence of Big Data, the Internet of Things, and artificial intelligence in the workplace" (A. K. Agarwal, Gans, and Goldfarb, 2017). This data is being used; however, employees have no insight into what data is being collected, how it is used, whether the data is used in promotions or terminations, whether the data can lead to discrimination, and what happens to one's data after termination. Employers do not disclose these details because they do not want employees to beat the system. An innovative solution to drive transparency in data collection can be achieved with visual models showing where the data goes and what automated decision making is used for (D'Acquisto et al., 2015).

Functional Creep in Employee Data Usage

'Functional creep' occurs when more information than the necessary minimum is being monitored (Ball, 2010; Kofman, 2017). Storing and harnessing data from many sources is cheaper and easier than it ever has been. Although employee data can be used in firing decisions, it is unclear whether the data is deleted and erased if an employee voluntarily terminates their job. Employees tend not to be told what information is monitored so they cannot tailor their actions and do not know if they are on the watchlist or not (Jeske et al., 2015). Employers claim that employees are monitored to ensure the security of the company's



Source: TUC/BritainThinks

systems, but functional creep occurs when these same data points are used to measure performance through speed and correctness of work (Jeske et al., 2015; TUC, 2017; Kofman, 2017; Ball, 2010). E-monitoring warps the incentive of employees to complete their work with full accuracy and "doesn't take into account the realities of the job" (TUC, 2017). E-monitoring is a 'blunt tool' for performance measurement because tracking time needed to complete a task might not reward the employee for doing a thorough job (TUC, 2017).

Mission Creep

'Mission creep' is where employee data can be used for alternate uses than the existing data was collected for, for example used in a discriminatory manner (Kofman, 2017; Ball, 2010). The justification is that data has already been collected and is readily available, even if not used for its original intended purpose (Kofman, 2017; Ball, 2010). If data is already collected and stored, it can easily be put to other uses and abused. Given that the employees have no visibility into the surveillance process, they do not know if their employer has crossed the boundary of acceptable use. Ideally, organizations should control who has access to employee data, the form of access controls, what access an immediate manager has, and whether HR can access one's information for hiring and firing decisions (D'Acquisto et al., 2015). In reality, these information points are not shared and employees fear retaliation if they were to ask. Another example of mission creep is that managers are notified if one of their employees seems to be looking for their next job based on their search history or documents downloaded (Kofman, 2017; Ball, 2010, Bloomberg, 2020). The dark side of mission creep occurs when employers sift through employee data to find a reason to fire an employee and "find the one mistake you made if they wanted" (Kofman, 2017; Ball, 2010; TUC, 2017). This is a departure from the primary purpose of workplace data collection for the goal of systems security and performance monitoring.

IV. How Employees Demand Privacy

What aspects of surveillance need to be transparent?

Employers tend to not share insight into what data is collected because that can give employees the information needed to work around the system. Consequently, employees have no idea what the collected data is being used for. Employment agreements often require employees to waive their right to workplace privacy by allowing routine collection of information. Routine information collection is more invasive than circumstantial investigation, because the latter would require a special justification as to why a particular employee was singled out to be closely monitored, whereas routine data collection involves all employees at all times (Wicker, 2011). Wicker (2011) studied the effects of active versus passive surveillance, also termed as comprehensive versus random monitoring (Wicker, 2011; Chen et al., 2007). Active surveillance profiles certain categories of people through a pre-selection where the user is unaware and cannot explain their side of the story, while passive surveillance limits employees from experimenting for fear of triggering the suspicion of the system (Wicker, 2011). The cost of data collection and storage is exponentially reducing over time. Therefore, employers are easily able to collect more information than ever before. Employee data mining is problematic because it represents the power that the organization has over each employee, furthering the existing "asymmetry of power" (Introna, 2002). Traditional principles such as anonymization cannot solve this problem because the very premise of employee monitoring is to track which employees do not cover their fair share of work. Decentralized repositories for data from disparate sources are recommended (D'Acquisto et al., 2015). If employees were given insight into how the surveillance is carried out, they could use that information to endorse their current capabilities as high-performing employees.

Trade Unions

According to the Trades Union Congress (TUC), new forms of surveillance should be implemented in the workplace only after informing trade unions who have a fundamental right to be involved in the decision-making process (TUC, 2017). Long-Bailey from the Labor Party in the UK strives to minimize the always-on working habits by allowing employees to pause from their work emails after hours (Topping, 2020). She supports a short-term and long-term plan for up to 5 years which was outlined in a manifesto to drive collective bargaining and protect mental health (Topping, 2020). Some middle managers are tempted to embrace surveillance to monitor their employees, but then realize that their senior leadership is using the same technology to scrutinize them, so both front line employees and middle level managers are supportive of trade unions solving this problem. Hosting regular catch-up meetings for employees and their managers is a low-tech solution suggested by trade union representatives to solve the problem of assessing productivity, but makes it harder for managers to complete their own daily workload if they are constantly checking in with large teams (Bloomberg, 2020). Trade union reps also suggest a more regimented structure of work hours to be applied to surveillance such as only monitoring from 9-5pm, but that does not completely solve the problem of Orwellian surveillance and ignores the flexibility that remote workers possess. Introna (2000) argues for "organizational justice" in the era of a "pervasive net of surveillance" (Introna, 2000). Similarly, Chen et. al (2007) argue for "procedural and distributive justice" for employees (Chen et al., 2007). Justice includes the right for employees to use their personal social media sites to campaign about a union-supported cause (TUC, 2017). Trade unions approach justice by searching for solutions that allow remote employees to help their managers understand their ability to work independently without excessive monitoring (Bloomberg, 2020).

Regulations

Companies have been encouraged to consider ethical data collection to maintain trust with their employees, but they have continued implementing

excessive e-monitoring. Regulations are needed to enforce a baseline status quo. Over 65% of workers are concerned about discrimination stemming from unregulated surveillance (TUC, 2017). Surveillance for legitimate reasons such as system security is necessary (TUC, 2017). Regulations can enforce that only necessary data points are being collected, so employees can be assured that their interests are safeguarded by institutional means (TUC, 2017). Successful regulations are timeless to account for the dynamic technology environment, which is why they aim to be neutral to the particular technologies (Whitley, 2020). However, the Employment Practices Code can and should be up to date with emerging surveillance technologies (TUC, 2017). Budd and Colvin (2008) propose three indicators that allow employees to resolve trust issues around e-monitoring. These include efficiency of company resources, equality and anti-discrimination, and democratic decision-making processes. Regulations can serve as a vehicle to educate employees about their rights. Employee data only represents a part of their whole context, but employees need not justify their lives outside work, termed the "right to a private life" (TUC, 2017). Empowered remote employees prefer regulation that mandates information about e-monitoring initiatives before they are introduced, with a justification for their introduction, and a mandate that after-hours monitoring is illegal (TUC, 2017).

V. Framework to Access if Surveillance is Excessive

This paper has established that although employees resent and resist employee monitoring, employers do have justified business needs for a certain spectrum of surveillance. Now, I explore a framework to ensure that reasonable employee privacy is considered. The notion of contextual integrity is key to making this distinction (Brey, 2005). Work meetings over video conferencing software are not usually considered private from an employer but sustained intense surveillance of personal phone calls without a justified business need and without prior consent can be considered "prima facie violations of privacy" (ibid.). To determine if surveillance is excessive, both the context and the level of accountability need to be considered (ibid.). The contents of personal phone calls should not be monitored, even on work hours, because these moments are generally considered private outside the office environment, and thus should remain private even inside the remote office environment (ibid.). The hallmark of excessive surveillance is lack of control over one's personal situation. Control can be violated physically by monitoring movements, psychologically by a software snooping through confidential conversations, or if the employees cannot control the level of surveillance. These findings can be classified into an overall "operationalized notion of privacy" (Brey, 2005).

The current state of affairs in the regulatory landscape at the US state level includes a California law that aims to "protect its citizens against privacy infringement of any nature...employers digging into employees' privacy after working hours violate these rights and might be accused in a court of law for privacy infringement" (Genova, 2009). Connecticut requires sharing info about e-monitoring, but that is the only state with such a law (Nockleby, 2002). At a federal level, the Fourth Amendment is only for the government as an employer, so corporations have no obligation (Nockleby, 2002). For non-government employers, the Electronic Communications Privacy Act (ECPA) still does not cover employees because they accept the terms and conditions of using their employer's system (Nockleby, 2002). In the EU, GDPR covers employee data and requires Data Protection Impact Assessments (DPIAs) (ICO, 2018).

The Information Commissioner's Office has a Code for Employment Practices that recommends including the justification for surveillance, understanding its psychological reactions on workers, finding the least privacy invasive mechanism for monitoring, providing transparency on how data will be applied in decisions, and not using surveillance data for other undisclosed reasons such as performance bonuses (TUC, 2017). As the European Court of Human Rights rightly says "private life is a broad concept that does not stop at the door of the workplace" (TUC, 2017). Therefore, invasive monitoring of private social media data or personal email accounts would need to be adequately justified, and business intelligence systems should not be permitted to make automated hiring and firing decisions based on employee data points (TUC, 2017).

VI. Conclusion

The current Covid-19 global pandemic demonstrates that remote working has gained a lot of traction and is here to stay. Workplace surveillance is another layer atop the already delicate relationship between a manager and an employee. Flexible working is a gray area without any hard and fast boundaries between home and work. Remote working is highly desirable for employees who would otherwise have a long commute, need to relocate, or have other parallel priorities such as caring for a dependent or child at home. Remote working is extremely desirable but involves sacrificing personal privacy to endure 24/7 employee monitoring as the cost of this freedom. The dark side of remote working is that employees are excessively monitored in the name of security of company-confidential information, but the data collected can be repurposed for electronic performance monitoring (EPM) (Jeske et al., 2015). The system is imbalanced in terms of power because employees are punished from their monitored data, but not rewarded. A recommended solution is using performance rewards as an incentive mechanism to drive employee acceptance of monitoring technology so both employers and employees can reap the benefits of surveillance data together (ibid.).

Bhave et al. (2020) term this "emerging entanglement of privacy contexts" (ibid.) where data privacy and physical privacy in the office are intertwined. The double-edged sword of remote working is that the same technological solutions that allow remote working also enable employee monitoring. The literature suggests possible solutions from the employer's end such as blocking access to inappropriate websites on work laptops, co-creating

employee monitoring systems with the perspective of employees designed into the system, and from the employee's end by encouraging end-to-end email encryption (Nockleby, 2002). I argue that remote employee acceptance of surveillance depends on the following factors - transparency on data collection from employers, clarification of data usage for system security or for hiring and firing decisions, and the avenues available for employee privacy concerns to be heard.

References

Agarwal, A., Gans, J., Goldfarb, A. (2017) "What to expect from artificial intelligence" MIT Sloan Management Review (58:3) pp. 23-27.

Allen, M., Coopman, S., Hart, J., Walker, K. (2007) "Workplace surveillance and managing privacy boundaries" Management Communication Quarterly (21) pp. 172-200.

Ball, K. (2010) "Workplace Surveillance: an overview" Labor History (51:1) pp. 87-106.

Bhave, D. P., Teo, L. H., Dalal, R. S. (2020) "Privacy at Work: A Review and a Research Agenda for a Contested Terrain" Journal of Management (46:1) pp. 127–164. https://doi.org/10.1177/0149206319878254

Bloomberg.com (2020) "Bosses Panic-Buy Spy Software To Keep Tabs On Remote Workers" [online] Available at: <https://www.bloomberg.com/news/features/2020-03-27/bosses-panic-buy-spy-software-to-keep-tabs-on-remote-workers> [Accessed 29 March 2020].

Bowcott, O., Rawlinson, K. (2017) "Romanian whose messages were read by employer had privacy breached" Guardian September 5. Retrieved from https://www.theguardian.com/law/2017/sep/05/romanian-chat-messages-read-by-employer-had-privacy-breached-court-rules.

Brey, P. (2005) "The Importance of Privacy in the Workplace" Privacy in the Workplace (eds. S. O. Hansson and E. Palm), Fritz Lang, pp. 97-118.

Budd, J. W., Colvin, A. J. (2008) "Improved metrics for workplace dispute resolution procedures: Efficiency, equity, and voice" Industrial Relations: A Journal of Economy and Society (47) pp. 460-479.

Chen, J., Ross, W. (2007) "Individual differences and electronic monitoring at work" Information, Community and Society (10:4) pp. 488-505, DOI: 10.1080/13691180701560002

Culnan, M.J. and Williams, C.C. (2009) "How Ethics Can Enhance Organizational Privacy: Lessons from the Choicepoint and TJX Data Breaches" MIS Quarterly (33:4) pp. 673- 687

D'Acquisto, G., Domingo-Ferrer, J., Kikiras, P., Torra, V., Montjoye, Y., Bourka, A. (2015) "Privacy by design in big data: An overview of privacy enhancing technologies in the era of big data analytics" 10.2824/641480.

Genova, G. (2009) "No Place to play: Current employee privacy Rights in Social Networking Sites" Business Communication Quarterly pp. 97-103.

Holmes, A. (2020) "Employees At Home Are Being Photographed Every 5 Minutes By An Always-On Video Service To Ensure They're Actually Working — And The Service Is Seeing A Rapid Expansion Since The Coronavirus Outbreak" [online] Business Insider Available at: <https://www.businessinsider.com/work-from-home-sneek-webcam-picture-5-minutes-monitor-video-2020-3?r=USandIR=T> [Accessed 29 March 2020].

Horton, C. (2020) "Employee Tracking: Why Workplace Tech Demands Trust" [online] Raconteur. Available at: <https://www.raconteur.net/business-innovation/employee-tracking-workplace-tech> [Accessed 28 March 2020].

Hyman, J. (2017) "A legal firing for fire chief's fiery posts" Workforce. Retrieved from https://www.workforce.com/2017/05/02/legal-firing-fire-chiefs-fiery-posts/.

Ico.org.uk. (2018) "Data Protection Impact Assessments (Dpias) Guidance" [online] Available at: <https://ico.org.uk/about-the-ico/ico-and-stakeholder-consultations/data-protection-impact-assessments-dpias-guidance/> [Accessed 10 April 2020].

Jeske, D., Santuzzi, A. (2015) "Monitoring what and how: Psychological implications of electronic performance monitoring" New Technology, Work and Employment (30) pp. 62-78. 10.1111/ntwe.12039.

Klopfer, P., Rubenstein, D. (1977) "The concept privacy and its biological basis" Journal of Social Issues (33) pp. 52-65.

Kofman, A., (2017) "The FBI Is Building A National Watchlist That Gives Companies Real-Time Updates On Employees" [online] The Intercept. Available at: <https://theintercept.com/2017/02/04/the-fbi-is-building-a-national-watchlist-that-gives-companies-real-time-updates-on-employees/> [Accessed 10 April 2020].

Nockleby, J., (2002) "Privacy In The Workplace" [online] Cyber.harvard.edu. Available at: <https://cyber.harvard.edu/privacy/Module3_Intronew.html> [Accessed 10 April 2020].

Nord, G., McCubbins, T., Nord, J. (2006) "E-Monitoring in the Workplace: Privacy, legislation, and surveillance software" Commun. ACM. (49) pp. 72-77. 10.1145/1145290.

Introna, L. (2000) "Workplace surveillance, privacy, and distributive justice" ACM SIGCAS Computers and Society (30) 10.1145/572260.572267.

Ozdemir, Z., Smith, H., Benamati, J. (2017) "Antecedents and outcomes of information privacy concerns in a peer context: An exploratory study" European Journal of Information Systems (26) 10.1057/s41303-017-0056-z.

Parks, R., Xu, H., Chu., C., Lowry, P. (2017) "Examining the intended and unintended consequences of organisational privacy safeguards" European Journal of Information Systems (26:1) pp. 37-65.

Pigni, F., Bartosiak, M., Piccoli, G., Ives, B. (2018) "Targeting Target with a 100 million dollar data breach" Journal of Information Technology Teaching Cases (8) pp. 9-23

Smith, W., Tabak, F. (2009) "Monitoring Employee E-mails: Is there Any Room for Privacy?" Academy of Management pp. 33-48.

Wicker, S. (2011) "Cellular telephony and the question of privacy" Commun. ACM (54:7) pp. 88–98. DOI:https://doi.org/10.1145/1965724.1965745

Stone-Romero, E., Stone, D., Hyatt, D. (2003) "Personnel selection procedures and invasion of privacy" Journal of Social Issues (59) pp. 343-368.

Topping, A. (2020) "Give People Right To Ignore Work Emails At Home, Says Long-Bailey" [online] The Guardian. Available at: <https://www.theguardian.com/politics/2020/feb/07/rebecca-long-bailey-labour-leadership-workers-rights-phones> [Accessed 29 March 2020].

Tuc.org.uk. (2017) "I'll Be Watching You" [online] Available at: <https://www.tuc.org.uk/research-analysis/reports/ill-be-watching-you> [Accessed 29 March 2020].

Vatcha, A. (2020) "Amy Vatcha: Employee Monitoring" [online] Available at: <https://apps.lse.ac.uk/mahara/view/view.php?id=2517> [Accessed 10 April 2020].

Whitley, E. (2020) "Week 5 Lecture: A Role for Technology? Approaches: How can we research Data Governance?" [online] LSE. Available at: <https://moodle.lse.ac.uk/course/view.php?id=3548> [Accessed 10 April 2020].

iS
CHANNEL

Addressing the Challenges Facing Decentralized Identity Systems

Andrei Volkov

MSc Management of Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Decentralized identity management
Decentralized identifiers
Digital identity
Self-sovereign identity
Blockchain

ABSTRACT

With data breaches becoming an increasingly prominent topic within society, businesses have begun directing resources towards enhanced security systems, while governments have seemingly attempted to grant individuals more rights over their personal data. With the development of new data management systems, organizations have the opportunity to create technologies that enhance and not endanger the privacy of data owners (Nyst et al., 2016). This paper discusses the concept of a decentralized identifier (DID) system, which shifts the control of personal data from centralized entities to the identity owners themselves. It places a focus on user data privacy by leveraging distributed ledger technology. Although a DID system presents numerous opportunities for data protection, it must first overcome a number of obstacles before replacing its centralized counterpart. This paper addresses two key challenges that DID systems face: scalability and interoperability. The proposed solutions to the scalability challenge include the implementation of a second layer protocol atop the distributed ledger as well as a simplified user experience provided by a digital wallet application. Meanwhile, the key strategies for addressing the interoperability challenge include the use of a Universal Resolver, integration of distributed ledgers, and facilitation of compatible digital wallets and identity hubs. By addressing these challenges through collaborative efforts, developers may be one step closer to granting everyone control over their personal data.

Introduction

As our daily lives are now practically inseparable from the Internet, our identities have also rapidly shifted from the physical to the online space, forming digital identities. Typically, digital identities are stored and managed by centralized institutions. One of the key reasons for the use of centralized systems is that users give up some control of their personal data for the services that a centralized platform provides in exchange. As a result, the user can enjoy the platform's features in a cost and time-efficient manner, not having to worry about the security of her data as the company presumably promises state-of-the-art protection.

Recently, however, such a system has demonstrated several drawbacks concerning user privacy and security. The breach of Equifax, a credit-rating agency, exposed personal details of 147 million users, including their social security numbers, home addresses, credit card details, and driver's IDs (EPIC.org, 2019). The Cambridge Analytica scandal unveiled how the political consultancy utilized personal data of 87 million Facebook users who trusted the social network with their information (Confessore, 2018). Besides the security concerns with regards to hackers, users also relinquish their privacy to websites, which monetize personal data through third party targeted advertisements.

Due to the security concerns of existing digital platforms, new and improved systems must orient themselves around user data privacy. Technology can provide mechanisms that would protect an individual's identity, restrict access to unwarranted parties, and verify the validity of an identity to authorized parties, all while maintaining the identity owner's data private. One promising technology in the field of digital identity management is blockchain. In contrast to the existing centralized authorities, blockchain embraces a decentralized approach to data management. Instead of concentrating all the power in the hands of governments and commercial entities, blockchain offers users sovereignty over their own digital identities.

As the concept of decentralized identity management has gained much attention in recent years, with a number of projects currently going through development stages, it is necessary to address not only the opportunities that the technology presents but also the challenges that companies will face as they continue building and expanding their decentralized systems.

Corresponding Author
Email Address: volkovandreimail@gmail.com

This paper aims to advance the understanding of decentralized identity management by conducting a literature review of the challenges that the technology faces, while also imparting a set of potential solutions to address said challenges. Since the topic of decentralized identity management is nascent, the literature review will rely on primary sources in addition to available scholarly research. The primary sources comprise of white papers, blog entries from decentralized platform developers on GitHub, posts on community websites DIF and W3C, as well as individual developers' blogs and their companies' blog entries. To extend the findings of the literature review, the proposed solutions will be grounded via a case study through an examination of Microsoft's decentralized system, ION.

Current State of Decentralized Identity Systems

Digital Identities

An individual's digital identity is formed from a myriad of information that any given user provides to gain access to certain websites and services online. Since there are many interpretations of the concept, it is essential to define what a digital identity consists of. Nyst et al. (2016) argue that a digital identity consists of three factors: identification, authentication, and authorization. Identification covers the establishment of information about a user, which could include official documents provided by the individual (passports, SSNs) or an aggregate of data generated by the user through her use of online services (ibid, p. 8). Authentication addresses the assertion of the information provided in the identification step and usually requires authentication credentials (ibid, p. 9). Lastly, authorization determines which operations are granted to a user based on their identification and authentication (ibid, p. 9). Therefore, digital identity consists of all three requirements existing in a digital form.

Self-Sovereign Identity

As a result of the security and privacy concerns in centralized systems, researchers have called for a more user-centric approach to digital identity management. One such approach, self-sovereign identity (SSI), proposes a model where a user has complete control and ownership of her data, without having to rely on a centralized authority. The key requirements of an SSI include (1) user's total control of own data; (2) authentication, security, and privacy are provided by the system, with no need for a centralized entity; (3) complete portability of the data as required by the user; (4) transparency of changes to the data provided by the system (Abraham, 2017).

Decentralized Identifiers

Consequently, SSI has led to the conception of DID. DID is an identification system that assigns a "standard, cryptographically verifiable, globally unique and permanent identity" (Aydar et al., 2019) to a user, granting full control of the data to the identity owner and eliminating the need for a centralized authority. It operates through an association to an asymmetric key (a combination of a public and private key). Private keys, which are only seen and known by the identity owner, are associated with public keys, which can be seen by anyone with whom the identity owner interacts with. Thus, a user can verify her identity via DIDs to other users in the system, as well as receive and send any documents, without revealing any information about herself (ibid, p. 10). Such a system creates an environment of credibility, security, and privacy while also providing complete control of personal data to the identity owner. Yet, in order for a system of DIDs to exist, a distributed ledger technology, or blockchain, is required.

Blockchain for Digital Identity Management

Distributed ledger technology brings much promise to achieving a genuinely decentralized identity management system. Blockchain has several assets that make it ideal for a DID and satisfy the four aforementioned requirements of an SSI. First, as blockchain is distributed by its nature, it cannot be controlled by a centralized authority, granting full control of data to the user. Second, blockchain's "public-key cryptography and hashing" mechanism provides authentication of the identity holder while keeping her data private; the distributed ledger also prevents the possibility of a "single point of failure and denial of service attacks," providing security to the identity holder (ibid, p. 6). Third, the distributed ledger technology also accounts for the portability of data between various users/entities in the system. Finally, blockchain's immutability and transparency are crucial to spotting any changes to the data in the system.

Hence, a decentralized digital identity is at the core of blockchain, making the technology appealing for the creation of a DID system.

Digital Identity Management

It is useful to illustrate a possible scenario of how a blockchain-based DID system could operate, as exhibited by Microsoft in Figure 1 (Microsoft, 2018). Irina, a recent university graduate, wants proof of her degree to demonstrate it to future employers. The university provides her with a DID-signed diploma, which Irina then saves in her identity hub. This signifies that the university, a credential issuer, has authenticated Irina and verified her diploma, a credential, via a digital signature (Aydar et al., 2019). Now, Irina can grant partial access to her diploma to a potential employer, a verifier, via her digital wallet app, a user agent. The employer can then confirm the validity of the degree issued by the credential provider.

Such a system presents numerous benefits for all parties involved. Irina no longer has to reach out to the university every time a potential employer requests proof of her degree, which saves time and money, as some universities request additional payments for such a service in the current centralized system. More importantly, Irina now has control over her own degree and job applications, without

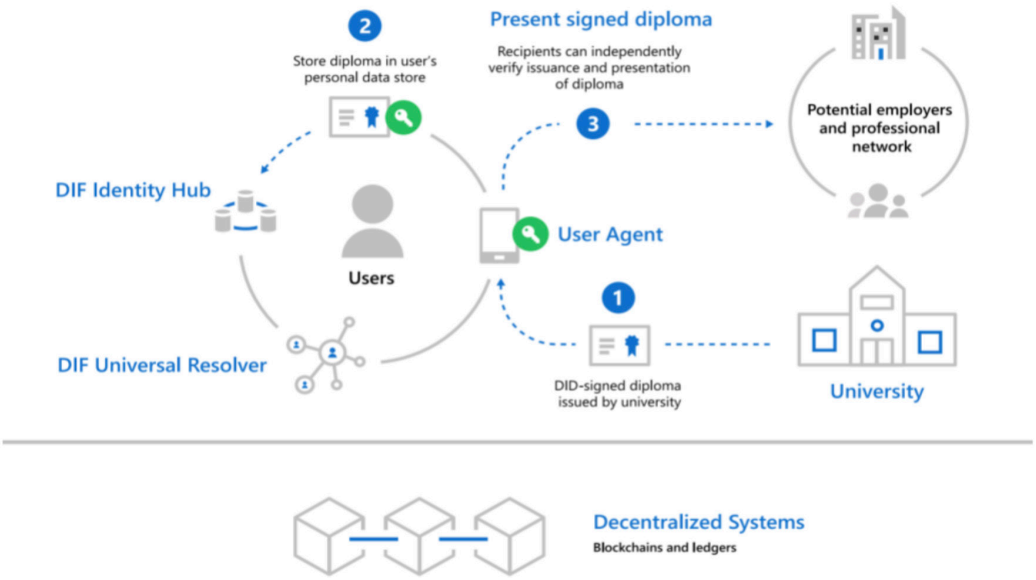


Figure 1: DID University Degree Example (Microsoft, 2018)

having to rely on her university. Furthermore, the university can no longer track what type of employer is checking the degree, which Irina may want to keep private. The university also benefits from time and cost-savings as it is no longer required to confirm the proof of degree for every student's potential employer request. The same could be said about the employer.

This simple case of a DID system could be expanded into a multitude of digital interactions that users may have. To enhance her own security and privacy, an identity owner could create multiple DIDs for all the possible interactions that she may have with other identity owners or institutions. Hence, if one DID is compromised, it does not affect other DIDs, keeping the user's identity and data protected (Aydar et al., 2019). Initially, each DID is an empty identity as it is not authenticated by any credential issuer; however, over time, DIDs gain credibility as more trusted parties assert the identity and information associated with the DID through a process of attestation (Microsoft, 2018). As a result, one could "require standard and verifiable claims from multiple trust providers before engaging in identity interactions and sensitive disclosures" (ibid, p. 15). Thus, the system also provides a level of trust amongst identity owners.

Challenges Facing DID Systems

Scalability

The issue of scalability is one of the most frequently cited challenges for blockchain, and distributed ledgers for DIDs are no exception. The challenge is two-fold as there are both technological and user adoption concerns. From a technological perspective, scalability can be interpreted as blockchain's ability to maintain its processing capabilities while expanding the network (Hileman and Rauchs, 2017). As the Bitcoin network grew, the time between the initiation of a transaction and its addition to the block extended to 10 minutes (Croman et al., 2016). Such a delay diminishes the throughput rate to 7 transactions/sec, which is minuscule compared to the average 2,000 transactions/sec of a centralized platform such as Visa, which at times achieves a rate of 56,000 transactions/sec (ibid, p. 1). This challenge becomes particularly relevant when projects such as Microsoft's ION set ambitious goals of providing a DID to 7.5 billion people (Microsoft, 2018). Without achieving at least parity with centralized systems, proponents of DIDs may find it difficult to convince the average consumer to switch over to a decentralized platform.

User adoption, therefore, is also a vital component of the scalability challenge. Besides the deterring slow transaction speeds of blockchain, the average user will also be reluctant to use DIDs due to the seemingly complex concept of the technology. Since a DID would primarily serve as a privacy and security solution, it is worth examining the current state of security maintenance by average users. According to an analysis of password breaches conducted in the UK, 55% of adults re-use the same password across multiple websites (NCSC, 2019). Hence, proposing DIDs to the average identity owner would be challenging, particularly if the DID platform's user experience is more complicated than a centralized system's process of creating a username and password.

Interoperability

Similar to scalability, interoperability is a common challenge across distributed ledgers, meaning DID systems will have to address the problem as well. The issue stems from the fact that seemingly identical distributed ledgers may have varying "security, integrity, and usability considerations" (Lesavre et al., 2020, p. 35), leading to difficulties in interactions across ledgers. Currently, the repository service GitHub contains over 6,500 blockchain-related projects, which utilize differing specifications, consensus mechanisms, and programming languages (Deloitte, 2018). Such a multitude of projects leads to a complex integration process amongst them. Furthermore, a research

study carried out by Hileman and Rauchs (2017) demonstrated that "only 25% of distributed ledger networks are interoperable with other distributed ledger networks and applications" (p. 74).

Thus, as it is highly unlikely that all users would utilize a single DID system, the question of interoperability becomes critical. A DID system's limited capability to only operate within the confines of its own distributed ledger would also drive down the user adoption rate.

Addressing DID Challenges

Scalability Solutions

Second Layer Protocol

Blockchain's slow throughput rate, as seen with Bitcoin transactions, is predominantly attributed to the block size and the block generation time (Croman, 2016). To amend this issue, the Bitcoin community has frequently proposed to increase the size of the blocks. DID research, however, has shifted the issue away from merely focusing on the block sizes and instead proposes for DID systems to operate on a blockchain as well as an additional protocol on top, the second layer protocol (Lesavre et al., 2020). The belief is that such a network would transfer transactions and operations away from the blockchain layer, alleviating the processing power, and providing more opportunities for scaling up (ibid).

An example of such a network is Microsoft's ION, a public and permissionless DID system which utilizes a second layer protocol called SideTree built atop of the Bitcoin blockchain (Simons, 2018). SideTree accelerates the throughput rate by bundling DID operations together into batches, instead of adding them individually onto the blockchain (ibid). SideTree's nodes process batches by adhering to predetermined rules that "enable them to independently arrive at the correct decentralized public key infrastructure state" (Buchner, 2020). Furthermore, SideTree nodes provide endpoints to carry out specific tasks, such as "create, resolve, update, recover, and deactivate," pertaining to DID documents (Tsai et al., 2020). The SideTree layer only utilizes the underlying blockchain's consensus mechanism to serialize the DID batches in a sequential and consistent manner (Buchner, 2020). Since SideTree does not require additional consensus mechanisms, it addresses the issue of small block sizes, as it is not encumbered by the underlying blockchain's limited transaction rate. After the protocol consolidates multiple operations into batches, it places the files in a distributed content-addressed storage, as seen in Figure 2 (Tsai et al., 2020). The only thing that is actually anchored to the blockchain itself is a reference to the batches (ibid). The batch data itself is stored as one. As nodes operate simultaneously while processing batches of DIDs, SideTree can run tens of thousands of operations per second (Simons, 2019).

The question of what is actually stored on the blockchain is also quite pertinent in matters of scalability. As seen in the SideTree protocol as well as other proposed DID systems (Aydar et al., 2019; Goodell and Aste, 2019), no personal data should be kept on the blockchain itself, even in an encrypted state. Not only is this vital for the security and privacy aspects of DID networks, but it also greatly benefits the system's scalability efforts. A second layer protocol makes this possible as no DID data has to overload the distributed ledger itself. Instead, only a reference or consent proof of said data is anchored to the blockchain. By utilizing a second layer protocol in this manner, ION is able to offload the operational

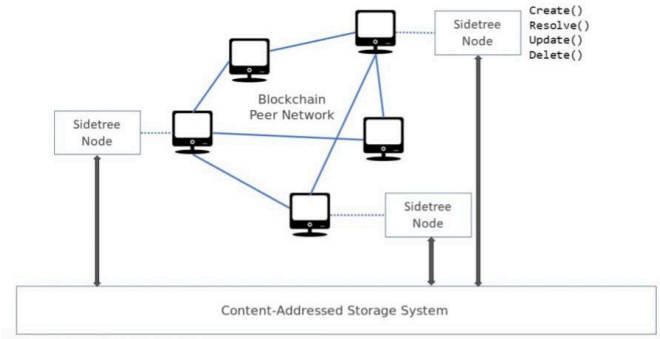


Figure 2: SideTree Protocol Architecture (Tsai et al., 2020)

burden from the underlying blockchain. As a result, the number of DID operations being processed at once increases drastically, expanding the overall capacity of the network. Thus, Microsoft's use of SideTree as the second layer protocol is an essential step towards achieving a truly scalable DID solution.

Digital Identity Wallet For Improved User Experience

In order to reach a large user base, a DID system not only has to achieve scalability via its technical specifications, but it also needs to present a flawless customer-facing solution. In its current state, a DID solution will fail to go beyond the 'innovators' phase of the Technology Adoption Cycle (Karlsson, 1988) as the system will be too complicated for the average user to understand. Even if the average user may see the value of privacy and security that a DID system provides, she will continue utilizing a centralized system due to its simplicity and familiarity. Thus, user experience is a vital feature of scalability.

The key to a satisfying user experience lies in a digital identity wallet, which takes the form of a phone and desktop application. The wallet serves as the primary and sole space where a user has to interact with the DID system. Through the wallet, a user should have access to her identifiers, private keys, and credentials, which are all only visible to her (Lesavre et al., 2020). The app also serves as space for users to interact with one another. Through the wallet, users send authentication requests, trusted issuers verify users and send credentials, and third parties can access credentials that are granted by the users. To simplify experience further, APIs could be used to trigger particular operations within the network, which could be easily initiated by a user scanning a QR code, a function already implemented by a DID start-up CryptId (Jacobovitz, 2016). Users should also be able to generate new identifiers

directly on the app, offline, without having to rely on a centralized authority to provide it for them (Lesavre et al., 2020). Such a feature is also beneficial for scalability since the blockchain would not be strained with facilitating operations for identifier generation. To further simplify access to the wallet, users could be asked to provide biometrics to sign onto the app, a feature that most smartphone providers allow.

Without a centralized authority, the responsibility of maintaining private keys falls onto the users. If a private key is lost or deleted, certain credentials could be lost forever, as the user does not have access to the equivalent of a 'forgotten password' option since there are no centralized authorities. In order to prevent this, developers of DID networks could include mechanisms such as "a custodian designated by the user, a list of user-appointed trustees, and time delay mechanisms, in the case of a private key being deleted" (Lesavre et al., 2020, p. 18). From this, it is interesting to note that the growth of the custodian market is inevitable. Just as with the storage of private keys on cryptocurrency exchanges, users will seek out custodians with the rise of DID networks. The DID purists, however, might argue that relying on custodians defeats the purpose of a decentralized system since the identity owner is, once again, relying on a mediator.

Microsoft's ION proposes a digital wallet, referred to as a User-Agent app (Microsoft, 2018). The purpose of the app is to "aid in creating DIDs, managing data and permissions, and signing/validating DID-linked claims" (ibid, p. 10). ION's ultimate goal is to create an app that would be accessible to the average user to the point where she would not even have to understand or see the term DID. Hence, DID network developers should approach their projects with the same mindset. Only a seamless app experience will comfort the user in the transition from a traditional centralized platform to a DID network.

Interoperability Solutions

Universal Resolver

All DID networks have to implement solutions that would allow users to interact across platforms. The Universal Resolver, as proposed by the Decentralized Identity Foundation (DIF) (2020), is one such solution that would integrate multiple DID systems via a single resolver of DIDs. Thus, every DID system must incorporate application code that would link their own system's method for interpreting DID documents to the Universal Resolver (ibid). By doing so, DID systems would interact with one another via a ubiquitous interface, without having to adapt to each other's application specifications.

From a technical perspective, the Universal Resolver is able to read and communicate all types of DID documents via 'drivers' for each identifier class (Sabadello, 2017). As DIF operates via open-source platforms, developers continuously contribute their DID drivers to the network, allowing the Universal Resolver to comprehend a vast number of DID documents (ibid). As these drivers have a direct connection to their own distributed ledger's nodes, the resulting network is blockchain-agnostic (ibid). This means that no matter the underlying blockchain that is used in a particular DID system, be it Sovrin, Bitcoin, or Ethereum, the Universal Resolver can process their documents and allow the systems to communicate with one another, without burdening them to fetch each other's technical specifications.

With the help of DIF's Universal Resolver, Microsoft's ION will allow the users of its digital wallet app to look up, authenticate, and request identifiers from users operating on all other DID systems (Microsoft,2018). Thus, in a scenario where a trusted entity sends a credential to a user, the credential's associated DID is processed via one of the drivers registered on the Universal Resolver, which then fetches the corresponding DID document (ibid). Such an interoperable system would create an all-around comprehensive directory of DIDs, allowing users to send and receive documents regardless of what DID systems their digital wallets operate on. Thus, the interoperability feature would also contribute to DID systems' scalability efforts, as average users would be inclined to adopt the technology only if there was a significant presence of other users and trusted entities utilizing it.

Integration of Distributed Ledgers

Another worthwhile interoperability solution is the cross-integration of ledgers. Here, the concept is to integrate competencies and features of one system into another. For example, various distributed ledger providers have integrated Hyperledger Indy's DID capabilities into their own systems. Cordenity, a smart contract created by the Corda Platform, implemented Hyperledger Indy's libraries into its own blockchain (Kopnin et al., 2020). According to Corda, the reasoning behind this integration is that "while Corda is best suited for developing decentralized applications for managing complex inter-organizational workflows, Indy is the leading open-source platform for self-sovereign identity" (ibid). Thus, Corda's smart contract operations rely on the credentials and documents that are authenticated by Indy's DID system.

Interoperable Digital Wallets & Identity Hubs

Due to various advantages and specializations of some DID systems over others, users and entities are likely to use varying digital wallets. To meet the identity owners' expectations and improve their user experience, developers of DID systems should consider facilitating interoperable digital wallets. Not only would the interoperable wallets allow users to manage their own private and public keys easily, but it would also ease the user authentication and credential transfer process for entities operating on differing DID systems. Developers could use protocols such as BIP-32, which facilitate the interoperability amongst digital wallets for cryptocurrency storage and management, as inspiration for the convergence of DID wallets (Maxwell et al., 2019).

Concluding Remarks

The aim of this paper was to further the understanding of the challenges and opportunities of DID systems via a literature review supported by a case study. The review highlights a number of findings related to decentralized identity management. The proponents of enhanced security and privacy in the digital space have to consider ways in which they could prioritize the interests of identity owners, granting them control over their personal data. The development of a network of DID systems is a step in the right direction. To address the challenges of scalability and interoperability, as well as numerous other obstacles, the developers of DID systems should seek collaborative efforts via open-source platforms. Additionally, in order to successfully implement DID networks into our digital ecosystem, DID advocates must clearly illustrate its advantages to the identity owners as well as businesses. This paper explored user adoption from the average identity owner's perspective. Hence, future research could examine the possible solutions to increasing adoption rates of DID systems from governmental and business perspectives.

References

Abraham, A. (2017). E-Government Innovationszentrum Whitepaper about the Concept of Self-Sovereign Identity including its Potential. www.egiz.gv.at

Aydar, M., & Ayvaz, S. (2019). Towards a Blockchain Based Digital Identity Verification, Record Attestation and Record Sharing System. http://arxiv.org/abs/1906.09791

Buchner, D. (2019). Decentralized Identity. GitHub. https://github.com/decentralized-identity/identity-hub/blob/master/explainer.md

Buchner, D. (2020). DID Method implementation using the Sidetree protocol on top of Bitcoin. GitHub. https://github.com/decentralized-identity/ion

Confessore, N. (2018). Cambridge Analytica and Facebook: The Scandal and the Fallout So Far. The New York Times. https://www.nytimes.com/2018/04/04/us/politics/cambridge-analytica-scandal-fallout.html

Croman, K., Decker, C., Eyal, I., Efe Gencer, A., Juels, A., Kosba, A., Miller, A., Saxena, P., Shi, E., Gün Sirer, E., Song, D., Wattenhofer, R., & Tech, C. (n.d.). On Scaling Decentralized Blockchains (A Position Paper) Initiative for CryptoCurrencies and Contracts (IC3) 1 Cornell.

Electronic Privacy Information Center. (2018). Equifax Data Breach. EPIC.Org. https://epic.org/privacy/data-breach/equifax/

Goodell, G., & Aste, T. (2019). A Decentralized Digital Identity Architecture. In Frontiers in Blockchain (Vol. 2, p. 17). https://www.frontiersin.org/article/10.3389/fbloc.2019.00017

Hileman, G., & Rauchs, M. (2017). Global Blockchain Benchmarking Study. Cambridge Center for Alternative Finance.

Holmes, A. (2019). Biggest hacks and data breaches of 2019: Capital One, WhatsApp, iPhone - Business Insider. Business Insider. https://www.businessinsider.com/biggest-hacks-and-data-breaches-of-2019-capital-one-whatsapp-iphone-2019-9?r=US&IR=T

Jacobovitz, O. (2016). Blockchain for Identity Management. The Lynne and William Frankel Center for Computer Science Department of Computer Science, Ben-Gurion University

Karlsson, C. (1988). Innovation adoption and the product life cycle. In Umeæ Economic Studies (Issue 185). http://www.diva-portal.org/smash/get/diva2:792156/FULLTEXT01.pdf%0Ahttp://hj.diva-portal.org/smash/record.jsf?pid=diva2:36369

Kopnin, A., Koren, A., & Vodopian, D. (2020). Combination of Hyperledger Indy and Corda. GitHub. https://github.com/Luxoft/cordentity

Lesavre, L., Varin, P., Mell, P., Davidson, M., & Shook, J. (2020). A Taxonomic Approach to Understanding Emerging Blockchain Identity Management Systems. https://doi.org/10.6028/NIST.CSWP.01142020

Maxwell, G., Reiner, A., Lombrozo, E., & Caldwell, M. (2019). Hierarchical Deterministic Wallets. GitHub. https://github.com/bitcoin/bips/blob/master/bip-0032.mediawiki#Abstract

Microsoft. (2018). Decentralized Identity. https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RE2DjfY Microsoft. (2018). Decentralized Identity.

NCSC. (2019). Most hacked passwords revealed as UK cyber survey exposes gaps in online security. National Cyber Security Centre. https://www.ncsc.gov.uk/news/most-hacked-passwords-revealed-as-uk-cyber-survey-exposes-gaps-in-online-security

Nyst, C., Makin, P., Pannifer, S., & Whitley, E. (2016). Digital Identity: Issue Analysis Executive Summary. www.chyp.com

Othman, A., & Callahan, J. (n.d.). The Horcrux Protocol: A Method for Decentralized Biometric-based Self-sovereign Identity.

Reed, D., Sporny, M., & Sabadello, M. (2020). Decentralized Identifiers (DIDs). In W3C. https://www.w3.org/TR/did-core/#dfn-did-documents

Richardson, B., & Waldron, D. (2019). Combating synthetic identity fraud | McKinsey. https://www.mckinsey.com/business-functions/risk/our-insights/fighting-back-against-synthetic-identity-fraud

Sabadello, M. (2017). A Universal Resolver for self-sovereign identifiers. Medium. https://medium.com/decentralized-identity/a-universal-resolver-for-self-sovereign-identifiers-48e6b4a5cc3c

Sadabello, M. (2017). Universal Resolver. GitHub. https://identity.foundation/

Schatsky, D., Arora, A., & Dongre, A. (2018). Reaping value from blockchain applications. Deloitte. https://www2.deloitte.com/us/en/insights/focus/signals-for-strategists/value-of-blockchain-applications-interoperability.html

Simons, A. (2019). Toward scalable decentralized identifier systems. Microsoft. https://techcommunity.microsoft.com/t5/azure-active-directory-identity/toward-scalable-decentralized-identifier-systems/ba-p/560168#

Sovrin. (2020). Innovation Meets Compliance. The Sovrin Foundation.

Swan, M. (2015). Blockchain for a New Economy. O'Reilly Media.

The, F., & Internet, D. (n.d.). Decentralized Identity - What Lies Ahead of Us: The Open(Interesting) Research Issues. https://en.wikipedia.org/wiki/On_the_Internet,_nobody_knows_you%27re_a_dog

Tsai, H. (2020). Sidetree Protocol Specifications. GitHub. https://github.com/decentralized-identity/sidetree/blob/master/docs/protocol.md

Yli-Huumo, J., Ko, D., Choi, S., Park, S., & Smolander, K. (2016). Where Is Current Research on Blockchain Technology?—A Systematic Review. PLOS ONE, 11(10), e0163477. https://doi.org/10.1371/journal.pone.0163477

iS
CHANNEL

Big Data in Smart Cities: A Critical Literature Review

Lisa Schaefer

MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Big Data
Smart Cities
Bounded Rationality
Social Embeddedness

ABSTRACT

Population growth, urbanisation and climate change are some of today's most significant challenges. Deploying big data and technologies to cities can potentially mitigate the countless problems faced by society. However, regardless of the numerous opportunities, concerns are being raised regarding data biases, privacy and the increase in surveillance. This literature review aims to assess the existing research on the topic of big data in smart cities in a critical manner to showcase divergences by scrutinising the topic from various perspectives. First, arguments underpinned by the bounded technical-rational view are outlined, including technical possibilities and best practice examples of smart cities. Attention then turns to socially embedded assumptions, questioning the overall utility of smart city initiatives. In conclusion, this review reveals an area for further research to explore: leveraging big data in smart cities to benefit all stakeholders.

1 Introduction

T Big data in smart cities provokes both utopian and dystopian rhetoric (Boyd and Crawford, 2012; Shin and Choi, 2015). On the one hand, an idealistic, almost hyperbolic, view of big data is being drawn in the literature. The phenomenon, framed as a revolutionary technical tool, leverages data for the generation of novel and unique insights, creating significant opportunities not only for businesses but also for public organisations and entire societies (Boyd and Crawford, 2012; Frith, 2017). Urban researchers extensively outline the possibilities of big data and analytics, drawing a utopian world of data-driven, highly efficient cities (Frith, 2017). On the other hand, several scholars build on the socio-technical school of thought and provide a more nuanced view of big data and smart cities by including political and societal dimensions. Some even present a dystopian view on data-driven cities by highlighting various implications (Kitchin, 2014b; Shin and Choi, 2015).

This review aims to critically assess the current literature on big data in smart cities to identify different points of contention regarding the use of big data in urban environments. Smart cities are predominantly seen as a holistic concept and a socio-technical phenomenon (Albino et al., 2015). This review, therefore, follows the definition by Bakici et al. (2012) describing a smart city as an "high-tech intensive and advanced city that connects people, information and city elements using new technologies in order to create a sustainable, greener city, competitive and innovative commerce, and an increased life quality" (ibid.). To reveal the utopian and dystopian view of big data in smart cities, the interests of various stakeholders as well as the divergences, the topic is scrutinised from multiple perspectives with their underlying assumptions.

First, the literature underpinned by the bounded technical-rational view is analysed, including its engineering and managerial rationality. The perspectives focus on technological aspects and best practices. Second, the underlying assumptions and arguments made by scholars within the literature of the socially embedded view are examined, including more reflective and questioning stances (Avgerou, 2019). As few scholars have followed a formal-technical rational approach to explore the topic of big data and smart cities, this perspective is only briefly discussed. Finally, the conclusion summarises the different perspectives and highlights relevant research gaps. Because of the interdisciplinarity of the topic, 21st-century, peer-reviewed articles were examined not only in the fields of information systems and management but also in cities, urban technology and government. To identify relevant papers, keywords in conjunction with smart cities* such as big data, Internet of Things, citizen centricity*, social* and privacy were selected to search the LSE Library Database, ABI/INFORM Database and Google Scholar. Articles were classified as relevant if the main topic was related to big data in smart cities and if one or more of the perspectives mentioned above were addressed. For the final selection, research papers not adding variety were rejected.

2 Bounded technical-rational perspectives

Whereas the formal technical-rational approach looks for an optimal solution, the bounded technical-rational view accepts satisfactory results due to various restrictions, such as the limited cognitive abilities of practitioners, information (un)availability, uncertainty and complexity (Avgerou, 2019). In the following section, the underlying assumptions

Corresponding Author
Email Address: lkschaefer@posteo.org

within the bounded technical-rational perspective are examined and contrasted.

2.1 Engineering rationality: Leveraging big data to build a smart city

The literature within engineering rationality focuses on the prominent assumption that with sufficient technology, cities' efficiency and the citizens' quality of life can be enhanced (Stone et al., 2018). The academic discourse sees information communication technology (ICT) as a core component and emphasises the importance of big data in smart cities as it is seen as a key enabler for data-driven urban projects. Valuable real-time insights are revealed and provide endless possibilities (Al Nuaimi et al., 2015; Kitchin, 2014b). The emerging literature characterises big data as being high in volume, velocity and variety (Kitchin, 2014b). Scholars enumerate various sources for big data in cities, including the Internet of Things (IoT) and data gleaned from surveillance or provided by citizens. Furthermore, the authors highlight the necessity to connect and integrate data sources to enable data analytics and derive valuable insights (Aguilera et al., 2017; Hashem et al., 2016; Kitchin, 2014b). It is important to note that smart city literature predominantly focuses on leveraging data generated by the IoT.

Some of the core notions underlying the academic discourse on smart cities have changed over the past decade. Specifically, the integration of IoT data and other sources was seen as a prominent technological challenge (Su et al., 2011). However, due to recent technological advances, platforms and cloud-computing now offer solutions to overcome the integration issue (Al Nuaimi et al., 2015; Hashem et al., 2016; Stone et al., 2018). Some researchers even draw a futuristic, utopian picture of cities. By coining the terms 'instrumental rationality' (Mattern, 2013) and 'solutionism' (Morozov, 2013), the academics rather follow a more formal- than bounded-rational approach. The scholars argue that datafication and computation enable the seamless monitoring of a city. In addition, the authors claim that leveraging insights through data analysis would result in a flawlessly functioning city, eliminating all inefficiencies (Mattern, 2013; Morozov, 2013).

However, despite technological advances, most researchers (Degbelo et al., 2016; Frith, 2017; Kitchin, 2014b) continue to recognise significant challenges, opposing the picture drawn by Mattern (2013) and Morozov (2013). Frith (2017) stresses the importance of formatting and analysing data through algorithms; otherwise, data will not reveal valuable insights. The challenge of data management and the harmonisation of various data formats is also addressed by Al Nuaimi et al. (2015) and Hashem et al. (2016). Both researchers claim that advanced algorithms and enormous computational power, which do not yet exist, are required to handle the complexity of data. This view is shared by Kitchin (2014b), who argues that although algorithms may conduct some data analysis, many processes still require human analysts, particularly concerning interpretation. Given these realities, Frith (2017) notes the importance of employing educated professionals, equipped with a sufficient understanding of metadata and database structure, to undertake these tasks. The author highlights that little research has been conducted on how employees interpret data and on which bases decisions are reached.

In conclusion, the literature outlines the available technologies and tools to enhance the efficiency and the quality of life within cities. However, the majority of academics continue to see technical limitations and the need for human involvement, supporting the bounded-rational rather than the formal-rational view of smart cities.

2.2 Managerial rationality: Deriving at best practices

The literature underpinned by a managerial view explores practices and principles that can be followed, defined by rational techniques, to achieve a desirable objective (Avgerou, 2019). The literature includes several case studies of smart city initiatives to derive best practices for city planners, endeavouring to overcome the technological challenges. Frameworks and roadmaps are created, ensuring seamless development and implementation of smart city initiatives with minimal cost involved. However, controversies in the academic discourse arise when scholars criticise best practices developed by corporations. It is claimed that these 'smart-city-in-a-box' solutions fail to prioritise the well-being of residents, suggesting a need for more citizen-centric practices (Aguilera et al., 2017; Kitchin, 2014b). Hereafter, the underlying arguments within the literature of the managerial rationality are outlined and contrasted to provide an overview of this perspective. Several researchers have conducted case studies of smart city projects, funded by corporations to frame best practices (Consoli et al., 2017; Cheng et al., 2015; Lee et al., 2014). Cheng et al. (2015) highlight that various studies have been performed regarding the implementation of sensors and data collection. However, the authors stress the need for flexible data platforms to leverage connected data. Hence, they investigated the platform CiDAP in Santander, Spain, to provide a design example of a data platform. The platform aims to analyse both historical and real-time data produced by over 2000 IoT devices within the city (Braun et al., 2018). Furthermore, best practices are outlined, including the management of multiple data sources and the support of data semantics. Consoli et al. (2017) re-direct the academic discourse towards the challenge of data integration, offering a government data model for smart cities. However, scholars note that the integration of data from heterogeneous sources remains problematic (Cheng et al., 2015; Lee et al., 2014).

In contrast, other researchers have taken a more holistic approach to smart cities, examining them as entire organisms (Ahlers et al., 2016). From this perspective, smart city initiatives conducted by corporations, and partly governments, are criticised as a top-down approach. While corporations often focus on their return on investment, the public sector is driven by increasing cities' attractiveness and economic stance, losing sight of the population's needs

(Alawadhi et al., 2012; Kitchin, 2014a). Ahlers et al. (2016) promote the active involvement of inhabitants within the planning and development process following a bottom-up approach to understand the needs of the wider society. Although scholars agree with the underlying assumption of the importance of user-centricity, many fail to outline how this can be achieved (e.g. Ahlers et al., 2016; Gupta, Chauhan, and Jaiswal, 2019). Aguilera et al. (2017) and Degbelo et al. (2016) are some of the few scholars filling this research gap. The authors suggest practices to build smart cities by combining existing infrastructure and leveraging citizen-produced data. An open data city approach is applied, allowing for easy data access by various stakeholders, therefore serving not only smart city initiators but society as a whole.

Lastly, it is noted that few scholars have developed a strategic roadmap and holistic framework for smart city projects. Al Nuaimi et al. (2015) highlight that planning a smart city goes beyond standalone initiatives and projects. It involves the consideration of social and technological requirements and various stakeholder needs. The researchers offer a roadmap and practices to follow when planning a smart city; however, these remain superficial. In contrast, Lee et al. (2014) develop a more comprehensive framework by studying Seoul and San Francisco, considering both technological and institutional aspects. Overall, academic consensus shows the need for further case studies to create effective, holistic best practices for smart city development (Lee et al. 2014; Scuotto et al. 2016).

3 Socially embedded perspective: Implications for society

Academics focussing on the socially embedded view take a more reflective, philosophical perspective on the broader implications of leveraging data to connect cities. The potential consequences for society are evaluated, and occasionally, academics question smart city movements (Avgerou, 2019; Tierney, 2019). Considering the motivations behind smart city initiatives, the literature underpinned by the socially embedded perspective debates the various consequences and implications for urban residents.

The academic discourse questions the core notion of smart cities resulting in a higher quality of life. It is claimed that urban projects, often funded by multinational corporations, are primarily profit-driven rather than citizen-centric (Braun et al., 2018; Tierney, 2019). Not only is citizen-centricity scrutinised, but the literature furthermore highlights the jeopardy of corporation dependency, with the risk of a technological lock-in effect and the rise of companies' monopolistic power (Hill, 2013; Tierney, 2019). Hill, as cited in Kitchin (2014b), even presents a dystopian view, contending that deploying corporate smart city solutions leads to inefficiencies because the public relies on particular devices and systems. With rapid technological progress, these devices risk becoming outdated due to the fact that corporations in monopolistic positions might not have an incentive to upgrade their technology. By exemplifying the phenomenon of monopolies through Sidewalk Lab's partnership with the City of Toronto, Tierney (2019) extends the academic discourse. The futuristic picture of consistently monitored cities drawn by Mattern (2013) and Morozov (2013), as cited in Kitchin (2014b), is reflected by Tierney (2019). However, the author does not draw upon a utopian vision but instead describes a planned undertaking. The scholar's main concern lies with the transformation of personal and environmental data into an economic resource by Google's subsidiary Sidewalk Labs, the point being that Google aims to monetise the project through the sale of residents' personal information to advertisers. Furthermore, it is feared that data will be analysed to influence people's actions to Google's benefit. With novel insights about citizens, not only can Google sell its products more efficiently, but it can also adjust people's actions to increase their service utilisation (Tierney, 2019). The author raises apprehensions not only regarding the planned surveillance of citizens and privacy invasions but also regarding the implications of data analytics and data biases for society. However, these concerns are not only addressed in recent literature but have also been extensively discussed over the past decade (Boyd & Crawford, 2012; Kitchin, 2014b). Because data and the revealed insights lack objectivity, scholars stress the importance of restrictions and regulations regarding data collection and algorithmic profiling. It is argued that data biases and automated, data-driven decisions could lead to disturbing consequences for society, including discrimination, rising inequality and a dilution of democracy. The scholars fear that cities will be regulated by technology and multinational corporations (Beretta, 2018; Kitchin, 2014b; Tierney, 2019; Van Zoonen, 2016). Furthermore, the academics highlight reservations regarding the constant monitoring of cities, describing the danger of surveillance and a 'Big Brother society'.

The high significance of these matters is underlined by the fact that privacy and security concerns are one of the most contested topics within the socially embedded perspective (Gupta et al., 2019; Kitchin, 2014b). Van Zoonen (2016) criticises the bounded technical-rational approaches of smart city solutions, claiming that residents' privacy concerns are not considered. The author argues that, whereas the collection of impersonal data for service purposes causes hardly any disquiet, resistance is expected when personal data are utilised for surveillance purposes. Meanwhile, Braun et al. (2018) highlight the necessity to address privacy and security concerns, claiming that the benefits of smart cities will diminish if citizens refuse to participate in these initiatives. However, although several scholars emphasise the various challenges and concerns smart cities present for society, the academic discourse lacks solutions and guidance for public institutions to ensure citizens' data protection and safety and to preserve democracy.

4 Conclusion

This critical review explored the topic of big data in smart cities from two main perspectives—the bounded-technical and the socially embedded rationales—revealing the main points of contention. First, the paper outlined the possibilities of leveraging

big data and technology to create efficient cities, tackling today's challenges and improving citizens' lives. The best practices of various initiatives and were outlined, partly drawing a utopian view of cities. Second, the social implications of smart city projects were examined, highlighting concerns regarding the delusion of democratic processes, privacy and security, as well as the rising level of surveillance, provoking dystopian rhetoric. By evaluating the different perspectives, the conflicting aim of balancing the demand for open data and data-driven, connected cities, while maintaining citizens' privacy and preventing a world of surveillance, is highlighted. Experts hold opposing views on smart city initiatives, debating whether these are beneficial or harmful to society. The recent announcement of Google's intention to build a smart city district in Toronto has intensified the discussion. For example, whereas Zuboff calls the plans 'surveillance capitalism', urbanist Florida argues that the Sidewalk Labs initiative could increase Toronto's competitiveness and "propel Toronto into the top ranks of global cities" (Wakefield, 2019).

Whilst various projects on city transformation have arisen worldwide, many open questions and challenges remain. Further, research on the use of data in cities is required to develop smart city strategies serving all stakeholder needs, rather than exclusively accommodating those of multinational corporations or governments. Moreover, the decision-making processes of human interpretation or automated algorithms related to data biases require further investigation to ensure a non-discriminatory and democratic city. Privacy concerns need to be addressed, including ambiguities in data ownership and the use of data. Lastly, it is of importance to further investigate the phenomenon of surveillance, including its containment within regulations, to avoid citizens' resistance to smart city projects.

References

A Aguilera, U., Peña, O., Belmonte, O., & López-de-Ipiña, D. (2017). Citizen-centric data services for smarter cities. Future Generation Computer Systems, 76, 234–247. https://doi.org/10.1016/j.future.2016.10.031

Ahlers, D., Driscoll, P., Löfström, E., Krogstie, J., & Wyckmans, A. (2016). Understanding Smart Cities as Social Machines. In Proceedings of the 25th International Conference Companion on World Wide Web (pp. 759–764). International World Wide Web Conferences Steering Committee. https://doi.org/10.1145/2872518.2890594

Al Nuaimi, E., Al Neyadi, H., Mohamed, N., & Al-Jaroodi, J. (2015). Applications of big data to smart cities. Journal of Internet Services and Applications, 6(1), 25. https://doi.org/10.1186/s13174-015-0041-5

Alawadhi, S., Aldama-Nalda, A., Chourabi, H., Gil-Garcia, J. R., Leung, S., Mellouli, S., … Walker, S. (2012). Building Understanding of Smart City Initiatives. In 11th International Conference on Electronic Government (EGOV) (pp. 40–53). Kristiansand, Norway.

Albino, V., Berardi, U., & Dangelico, R. M. (2015). Smart Cities: Definitions, Dimensions, Performance, and Initiatives. Journal of Urban Technology, 22(1), 3–21. https://doi.org/10.1080/10630732.2014.942092

Avgerou, C. (2019). Notes on Lecture 1. London.

Beretta, I. (2018). The social effects of eco-innovations in Italian smart cities. Cities, 72, 115–121. https://doi.org/10.1016/j.cities.2017.07.010

Boyd, D., & Crawford, K. (2012). Critical questions for big data: Provocations for a cultural, technological, and scholarly phenomenon. Information Communication and Society, 15(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Braun, T., Fung, B. C. M., Iqbal, F., & Shah, B. (2018). Security and privacy challenges in smart cities. Sustainable Cities and Society, 39, 499–507. https://doi.org/10.1016/j.scs.2018.02.039

Cheng, B., Longo, S., Cirillo, F., Bauer, M., & Kovacs, E. (2015). Building a Big Data Platform for Smart Cities: Experience and Lessons from Santander. Proceedings - 2015 IEEE International Congress on Big Data, 592–599. https://doi.org/10.1109/BigDataCongress.2015.91

Consoli, S., Presutti, V., Reforgiato Recupero, D., Nuzzolese, A. G., Peroni, S., Mongiovi', M., & Gangemi, A. (2017). Producing Linked Data for Smart Cities: The Case of Catania. Big Data Research, 7, 1–15. https://doi.org/10.1016/j.bdr.2016.10.001

Degbelo, A., Granell, C., Trilles, S., Bhattacharya, D., Casteleyn, S., & Kray, C. (2016). Opening up Smart Cities: Citizen-Centric Challenges and Opportunities from GIScience. ISPRS International Journal of Geo-Information, 5(2), 16. https://doi.org/10.3390/ijgi5020016

Frith, J. (2017). Big Data, Technical Communication, and the Smart City. Journal of Business and Technical Communication, 31(2), 168–187. https://doi.org/10.1177/1050651916682285

Gupta, P., Chauhan, S., & Jaiswal, M. P. (2019). Classification of Smart City Research - a Descriptive Literature Review and Future Research Agenda. Information Systems Frontiers, 21, 661–685.

Hashem, I. A. T., Chang, V., Anuar, N. B., Adewole, K., Yaqoob, I., Gani, A., … Chiroma, H. (2016). The role of big data in smart city. International Journal of Information Management, 36(5), 748–758. https://doi.org/10.1016/j.ijinfomgt.2016.05.002

Kitchin, R. (2014a). The Governmental and Business Rationale for Big Data. The Data Revolution: Big Data, Open Data, Data Infrastructures & Their Consequences, 113–127. https://doi.org/10.4135/9781473909472.n7

Kitchin, R. (2014b). The real-time city? Big data and smart urbanism. GeoJournal, 79(1), 1–14. https://doi.org/10.1007/s10708-013-9516-8

Lee, J. H., Hancock, M. G., & Hu, M. C. (2014). Towards an effective framework for building smart cities: Lessons from Seoul and San Francisco. Technological Forecasting and Social Change, 89, 80–99. https://doi.org/10.1016/j.techfore.2013.08.033

Lombardi, P., Giordano, S., Farouh, H., Yousef, W., Lombardi, P., Giordano, S., … Yousef, W. (2012). Modelling the smart city performance. Innovation - The European Journal OfSocial Science Research, 25(2), 137–149. https://doi.org/10.1080/13511610.2012.660325

Scuotto, V., Ferraris, A., & Bresciani, S. (2016). Internet of Things Applications and challenges in smart cities: a case study of IBM smart city projects. Business Process Management Journal, 22(2), 357–367. https://doi.org/10.1108/BPMJ-05-2015-0074

Shin, D. H., & Choi, M. J. (2015). Ecological views of big data: Perspectives and issues. Telematics and Informatics, 32(2), 311–320. https://doi.org/10.1016/j.tele.2014.09.006

Stone, Merlin; Knapper, Jonathan; Evans, Geraint; Aravopoulou, E. (2018). Information management in the smart city. The Bottom Line, 31(3/4), 234–249. https://doi.org/10.1108/BL-07-2018-0033

Tierney, T. F. (2019). Big Data, Big Rhetoric in Toronto's Smart City. Architecture and Culture. https://doi.org/10.1080/20507828.2019.1631062

Van Zoonen, L. (2016). Privacy concerns in smart cities. Government Information Quarterly, 33(3), 472–480. https://doi.org/10.1016/j.giq.2016.06.004

Wakefield, J. (2019). Google given green light for Toronto smart city. BBC News. Retrieved from https://www.bbc.co.uk/news/technology-50234146

iS
CHANNEL

Social Media Personalization Algorithms and the Emergence of Filter Bubbles

Sanveer (Sunny) Rehani

MSc Management of Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Social media
Content personali-zation algorithms
Filter bubbles
Opinion polarization
Preference data
Platform governance

ABSTRACT

This article investigates how the technical infrastructure of social media platforms, particularly personalization algorithms, enables filter bubbles to emerge. It identifies several possible explanations, namely that platform owners intend this outcome; that the relevant algorithms contain inherent biases; and that user actions amplify the effect of these algorithms. While the true answer cannot be ascertained, the article concludes by outlining important areas for future research and highlighting the implications of social media content personalization.

I. Motivation

Content personalization on social media platforms is widely perceived as a beneficial feature, enabling each of us to have a unique and individualized online experience. What is seldom discussed is the hidden danger this carries: the continuous reinforcement of users' own viewpoints and beliefs. Without any exposure to content that chal-lenges existing viewpoints, it is easy for social media users to obtain a distorted image of the real world due to the limited scope of information that they encounter. This phenomenon, dubbed 'filter bubbles', could have a serious effect on our ability as individuals to form balanced opinions, and could negatively alter the way we react to opinions that contradict our own.

What makes these filter bubbles especially dangerous is our ignorance of their exist-ence. Social media platforms, in an effort to provide users with the content most rele-vant for them, conduct this personalization automatically without informing users. A concept known as "what you see is all there is" (Kahneman, 2011, p. 85) describes a cognitive bias faced by humans whereby we treat the information available to us as if it were the only information to exist, thus making judgements and decisions based solely on that information. When filter bubbles cause all the content that we see to align with our existing ideologies, it becomes evident that this cognitive bias could lead to false illusions of reality.

It is critical that we address the issue of filter bubbles sooner rather than later. As social media platforms are increasingly utilized as sources of news and information, and as data algorithms become more advanced, it seems inevitable that this problem will only worsen. If left unchecked, filter bubbles could propagate misinformation among online communities, therefore serving as a serious threat to democracy and contrib-uting further to a global society that is arguably more polarized and divided than ever before.

Corresponding Author
Email Address: sunny.rehani@gmail.com

II. Literature Review

This section distinguishes between two distinct streams of literature; one that focuses on the outcomes of content personalization, and another that focuses on the tech-nical design of the algorithms that enable content personalization. Together, these two streams comprise the context within which this paper's research is situated.

a. Research on consequences

There exists a vast amount of literature concerning the consequences of social media content personalization. Cass Sunstein pointed out the dangers of personalization as early as 2001, years before the ascent of social media, stating that the internet could "increase people's ability to wall themselves off from topics and opinions that they would prefer to avoid" (p. 202). In more recent literature, a recurring conclusion is that social media content personalization often results in ideological segregation to some degree.

A study by Dylko et al. (2018) demonstrates that the customizability technology em-ployed by popular social media platforms leads to increased selective exposure to at-titude-consistent content, thereby causing increased political polarization. Bakshy et al. (2015), in a study of over 10 million US Facebook users, discovered that "the risk ratio comparing the probability of seeing cross-cutting content relative to ideologically consistent content [on a user's 'News Feed'] is 5% for conservatives and 8% for liber-als" (p. 1131). The considerable majority of information that social media users are exposed to, then, is aligned with their existing beliefs. Additionally, Knobloch-West-erwick et al. (2015) show that source

credibility does not influence the impact of po-litical information on political attitude. This is especially noteworthy when discussing social media, as users share not only credible news articles but also opinion pieces. Flaxman et al. (2013) find that articles shared on social media are more ideologically segregating than news consumed directly from news sites, mainly due to opinion pieces.

A key limitation of this set of research is the difficulty and potential subjectivity in-volved in measuring the ideological slant of news sources or pieces of information. However, this weakness is overcome by the frequent recurrence of similar conclusions across the research field.

b. Research on technical elements

There is also an ample amount of literature concerning the technical elements of con-tent personalization. Often this research focuses on the recommender systems of e-commerce sites rather than social media platforms, but as these systems are similar in design, the literature is still useful in this context. Adomavicius and Tuzhilin (2005) classify recommender systems into three categories: content-based recommenders, which utilize users' past behavior to make recommendations; collaborative filtering recommenders, which make recommendations based on the behavior of other users with similar preferences; and hybrid systems, which combine these approaches. Col-laborative filtering is more widespread today, but social media platforms likely employ hybrid approaches to personalize content for users.

This personalization is most commonly enabled by 'item-item algorithms', which de-termine the 'distance' between items based on "how closely users who have rated these items agree" (Alaimo and Kallinikos, 2019, para. 8). This means that items are grouped together into neighborhoods when the same users tend to like or dislike them. The algorithm can then recommend items to users according to other items in the same neighborhood for which they have previously demonstrated a preference. In the context of social media, these items would largely consist of online content (e.g. articles) shared by users; for example, if the Facebook users who tend to 'like' Fox News articles shared on their feed also tend to 'like' Breitbart News articles shared on their feed, then Fox News articles and Breitbart News articles might be grouped into the same neighborhood.

Of course, the act of 'liking' is simply one form of preference data that can be fed into personalization algorithms. Alaimo and Kallinikos (2019) explain that explicit data is collected through "actions that can be straightforwardly linked to preferences" (para. 7), such as the aforementioned Facebook 'like'. Ekstrand et al. (2011) add that pref-erence data can also be collected implicitly from user behavior, e.g. by monitoring clicks, time spent on a page, and so on. Social media platforms presumably collect both kinds of preference data. However, implicit data contains more noise, i.e. mean-ingless information, than explicit data (O'Mahony et al., 2006), which may limit its accuracy in predicting user preferences.

This set of research is somewhat limited by its heavy focus on e-commerce, and rela-tive disregard for social media. While the systems are likely quite similar in any case, it is surprising that there is relatively little research on the technical elements of social media content personalization in particular, given the massive relevance of social me-dia in the modern world. Additionally, much of the research is rather outdated when considering how rapidly these algorithms are being refined and reworked.

c. The gap

Although these are two rich and plentiful streams of literature, it seems that there exists somewhat of a gap between them. There is much discussion on the outcomes of con-tent personalization, as well as on the design of personalization algorithms - but very little on how exactly the latter leads to the former. The aim of this paper is therefore to serve as the bridge between these two fields. This paper will seek to answer the question: *how does the technical infrastructure of social media platforms en-able the emergence of filter bubbles?*

III. Problem Analysis

The existing literature explored in the previous section gives us a good baseline from which we can begin to answer this question. Firstly, it will be helpful to examine why personalization algorithms are implemented into the infrastructure of social media platforms in the first place. It is important to note that today's social media monoliths had not employed any such algorithms in their early days. In fact, user feeds tended to be sorted chronologically. What this provided, from a user's perspective, was a clear finish line for browsing; users could scroll through the new content that had been posted since they were last online, and then stop. However, as these platforms rapidly became more popular, the rate at which digital information was being produced and shared grew exponentially, creating a problem of information overload (Bozdag, 2013).

Information overload causes stress, confusion, and cognitive strain (Eppler and Men-gis, 2004), and can even result in 'social media fatigue' (Bright et al., 2015). Platforms like Facebook, Twitter, and Instagram needed a way to combat this issue in order to keep their massive userbases engaged. Personalization algorithms were a solution that enabled the filtering of information to present only the content relevant to each user. This seems logical, and arguably even necessary, but still begs the question: how and why do these algorithms ultimately equate 'relevant' content to attitude-consistent con-tent?

We identify two possible explanations, both of which will be explored in the following subsections. The first is that social media platform owners are incentivized to inten-tionally program the algorithms in this way. The second – slightly more complex – explanation is that although the outcome is unintentional, it is enabled by inherent biases in the algorithms' design, as well as by the actions of users themselves.

a. Intended design?

One rationalization for the emergence of filter bubbles is the deliberate programming of personalization algorithms to predominantly present content that users are likely to agree with. Research has shown that disagreement in an online setting leads to negative emotion and aggression (Masullo Chen and Lu, 2017). It is safe to assume that plat-form owners, i.e. administrators, wish to avoid inciting these sentiments among their userbase due to the risk of losing user engagement. By extension, then, administrators are incentivized to minimize the level of disagreement occurring on their platform (Chitra and Musco, 2020). Cross-cutting content is naturally a major source of disa-greement and conflict and is thus undesirable to administrators. Therefore, administrators may purposefully implement algorithms designed to present less cross-cutting content and more attitude-consistent content.

Chitra and Musco (2020), in a study of Twitter and Reddit, demonstrate that when a network administrator is able to actively filter social content in an effort to present users with content that matches their beliefs, the measure of opinion polarization across that network increases significantly (i.e. filter bubbles emerge). This certainly gives some weight to the explanation discussed here.

b. Or a symptom of other factors?

It is also entirely possible that filter bubbles emerge inadvertently as a byproduct of other factors. Firstly, algorithms may not be as objective as we would like to believe. Gillespie (2014) argues that the functions performed by personalization algorithms "always depend on inscribed assumptions about what matters, and how what matters can be identified" (p.177). Human biases manifest themselves in the design of the algorithms that dictate what content we see and do not see. Social media companies are careful to declare these algorithms as neutral and objective, but in reality, this is neither true nor possible (Gillespie, 2014). Although our description of item-item al-gorithms in the previous section is relatively straightforward, this is a gross simplifica-tion of what is, in practice, an incredibly complex black-box technology. So complex, in fact, that the engineers behind them may not even fully understand what they have evolved into. Paul Haahr, an engineer at Google involved with ranking algorithms, has openly stated that Google does not fully comprehend the way in which its ranking system works (Schwartz, 2016).

A prime example of human biases being unwittingly ingrained into algorithms is given by Ananny (2011), who discovered when installing Grindr, a dating app for gay men, that the Android Market inexplicably suggested a sex offender locator app under the 'related' applications. It is possible that the algorithm employed by Android was able to "identify a subtle association that, though we may not wish it so, is regularly made in our culture, between homosexuality and predatory behavior" (Gillespie, 2014, p. 190). Perhaps, then, the emergence of filter bubbles is simply a reflection on a flawed human way of thinking that has unknowingly been embedded into personalization algorithms - that the information we agree with is the most relevant information.

Alternatively, filter bubbles may have more to do with the choices of users than with the technical infrastructure of social media platforms. Referring back to content-based recommenders, we can assume that personalization is at least partly based on the behavior of users. It is conceivable, then, that users may indeed initially be presented with a balanced range of content but choose only to engage with attitude-consistent content, thus conditioning the algorithm over time to present more attitude-consistent and less cross-cutting content. This theory is evidenced by Munson and Resnick (2010), who attempted to present more diverse content to challenge-averse people and found that information consumption habits were not significantly affected, regardless of the presentation method. Another study discovered that while over 95% of Face-book users are exposed to at least some amount of cross-cutting content in their feeds, less than 55% of users choose to engage with (i.e. click on) this content (Bakshy et al., 2015).

While user behavior is plausibly at least partly to blame, this selective exposure may in fact be exacerbated by the algorithm's ranking system. In a study of search engines, Joachims and Radlinski (2007) demonstrate a clear negative correlation between search result rank number and frequency of clicks (p. 35). Moreover, they use eye-tracking technology to show that over half of the time, users do not even look at results below the third rank (p.35). If we extrapolate this behavior to a social media context, we can infer that users will tend to ignore cross-cutting information if it is not displayed near the top of their feed. So, although personalization algorithms may indeed be including cross-cutting content, it may be futile if this content is presented significantly lower in the feed than attitude-consistent content.

IV. Facebook: a brief case study

Though the details of social media personalization tend to be kept confidential, Face-book has occasionally published informative blog posts on their 'Newsroom' or 'En-gineering' domains, i.e. their platforms for communicating with the public. These will allow us to examine the extent to which the concepts discussed here are manifesting in reality.

In a blog post titled "Recommending items to more than a billion people", Facebook reveals that they employ a collaborative filtering technique in order to recommend pages and groups to users (Kabiljo and Ilic, 2015). A separate post about a 'News Feed' revamp claims to "learn from you and adapt over time" (Mosseri, 2016, para. 5), indicating that content-based recommendation is utilized in their content ranking algorithm. This confirms our prior assumption that social media platforms adopt hy-brid approaches to personalization.

In the same post, Facebook asserts their impartiality, and later states that their "aim is to deliver the types of stories we've gotten feedback that an individual person most wants to see. We do this not only because we believe it's the right thing but also because it's good for our business." (Mosseri,

2016, para. 10). Interestingly, this lends itself to the theory that social media companies intentionally design personalization algorithms in a way such that ideological segregation is made inevitable.

Facebook also discusses their collection of preference data. As far as explicit data, they admit that identifying positive signals (e.g. 'liking', joining a group, etc.) is much more straightforward than negative signals. Regarding implicit data, they claim their ap-proach is to "treat the data as a combination of binary preferences and confidence values" (Kabiljo and Ilic, 2015, para. 38). In other words, their algorithm analyzes implicit signals (e.g. time spent viewing a post, etc.) to estimate the likelihood that a user will find a given recommendation useful, even when no explicit preference has been put forth. This is significant because it verifies that Facebook can infer more about users than what they are willing to divulge. That is, even if users make a con-scious effort to diversify their information consumption, these algorithms can still es-timate their ideological leaning based on implicit activities, and subsequently adjust the type of content they are exposed to in the future.

V. Conclusions

We have conducted an in-depth exploration of the way in which the technical infra-structure of social media platforms (specifically their personalization algorithms) ena-ble the emergence of filter bubbles. Several possible explanations were identified, namely that this outcome is intentional on behalf of platform owners; that the algo-rithms have unavoidable inherent biases; and that user decisions amplify the effect of the algorithms. Of course, the true answer remains unknown. These algorithms are trade secrets, and the chances of social media companies revealing their inner work-ings are slim.

This research has naturally been constrained by the lack of official documentation regarding these algorithms, but it has nonetheless shed light on a largely overlooked phenomenon that affects nearly everyone. Going forward, there should be more em-pirical research conducted to determine potential countermeasures to online filter bubbles. Munson et al. (2013) developed a browser widget that tracks a user's internet history and continually displays how ideologically balanced their information con-sumption is. This is a fascinating idea, and there should be further studies that explore a social-media-specific solution, given that people increasingly consume information in bite-sized amounts (i.e. tweets, Facebook statuses, news headlines) as they scroll through their feeds.

It is easy for some to disregard this issue, claiming that they use social media merely to keep in touch with friends and that they consume news and information elsewhere. The reality, though, is that social media platforms have reworked the fabric of the internet as a whole. Through social plugins (one-click widgets on other websites to 'like' content through your Facebook account, share content on your Twitter profile, etc.), social media and the external web are "becoming increasingly interconnected with each other, as the activities performed in one space will affect the other, rendering both more open and relational" (Gerlitz and Helmond, 2013, p. 1354). The implica-tion here is that no matter where on the internet one chooses to go, social media platforms are observing, learning, and personalizing.

References

Adomavicius, G., & Tuzhilin, A. (2005). Toward the next generation of recommender systems: A survey of the state-of-the-art and possible extensions. IEEE transactions on knowledge and data engineering, 17(6), 734-749.

Alaimo, C., & Kallinikos, J. (2019). Recommender systems.

Ananny, M. (2011, April 15). The Curious Connection Between Apps for Gay Men and Sex Of-fenders. Retrieved April 15, 2020, from https://www.theatlantic.com/technology/ar-chive/2011/04/the-curious-connection-between-apps-for-gay-men-and-sex-offenders/237340/

Bakshy, E., Messing, S., & Adamic, L. A. (2015). Exposure to ideologically diverse news and opin-ion on Facebook. Science, 348(6239), 1130-1132.

Bozdag, E. (2013). Bias in algorithmic filtering and personalization. Ethics and information tech-nology, 15(3), 209-227.

Bright, L. F., Kleiser, S. B., & Grau, S. L. (2015). Too much Facebook? An exploratory examina-tion of social media fatigue. Computers in Human Behavior, 44, 148-155.

Chitra, U., & Musco, C. (2020, January). Analyzing the Impact of Filter Bubbles on Social Net-work Polarization. In Proceedings of the 13th International Conference on Web Search and Data Mining (pp. 115-123).

Dylko, I., Dolgov, I., Hoffman, W., Eckhart, N., Molina, M., & Aaziz, O. (2018). Impact of cus-tomizability technology on political polarization. Journal of Information Technology & Poli-tics, 15(1), 19-33.

Ekstrand, M. D., Riedl, J. T., & Konstan, J. A. (2011). Collaborative filtering recommender sys-tems. Foundations and Trends® in Human–Computer Interaction, 4(2), 81-173.

Eppler, M. J., & Mengis, J. (2004). The concept of information overload: A review of literature from organization science, accounting, marketing, MIS, and related disciplines. The information society, 20(5), 325-344.

Flaxman, S., Goel, S., & Rao, J. M. (2013). Ideological segregation and the effects of social media on news consumption. Available at SSRN, 2363701.

Gerlitz, C., & Helmond, A. (2013). The like economy: Social buttons and the data-intensive web. New media & society, 15(8), 1348-1365.

Gillespie, T. (2014). The relevance of algorithms. Media technologies: Essays on communication, materiality, and society, 167, 167-193.

Joachims, T., & Radlinski, F. (2007). Search engines that learn from implicit feedback. Com-puter, 40(8), 34-40.

Kabiljo, M., & Ilic, A. (2018, December 3). Recommending items to more than a billion people. Retrieved April 22, 2020, from https://engineering.fb.com/core-data/recommending-items-to-more-than-a-billion-people/

Kahneman, D. (2011). Thinking, fast and slow. New York: Farrar, Straus and Giroux.

Knobloch-Westerwick, S., Johnson, B. K., & Westerwick, A. (2015). Confirmation bias in online searches: Impacts of selective exposure before an election on political attitude strength and shifts. Journal of Computer-Mediated Communication, 20(2), 171-187.

Masullo Chen, G., & Lu, S. (2017). Online political discourse: Exploring differences in effects of civil and uncivil disagreement in news website comments. Journal of Broadcasting & Electronic Media, 61(1), 108-125.

Mosseri, A. (2019, November 7). Building a Better News Feed for You. Retrieved April 24, 2020, from https://about.fb.com/news/2016/06/building-a-better-news-feed-for-you/

Munson, S. A., & Resnick, P. (2010, April). Presenting diverse political opinions: how and how much. In Proceedings of the SIGCHI conference on human factors in computing systems (pp. 1457-1466).

Munson, S. A., Lee, S. Y., & Resnick, P. (2013, June). Encouraging reading of diverse political viewpoints with a browser widget. In Seventh International AAAI Conference on Weblogs and Social Media.

O'Mahony, M. P., Hurley, N. J., & Silvestre, G. C. (2006, January). Detecting noise in recom-mender system databases. In Proceedings of the 11th international conference on Intelligent user interfaces (pp. 109-115).

Schwartz, B. (2016, March 8). Google's Paul Haahr: We Don't Fully Understand RankBrain. Re-trieved April 18, 2020, from https://www.seroundtable.com/google-dont-understand-rankbrain-21744.html

Sunstein, C. R. (2001). Republic.com. Princeton University Press.

iS
CHANNEL

Social Media as a Data Source in the Public Sector: Socio-Technical Challenges for Economic Indicators

Keisuke Idemitsu

MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Big data
Government
Public sector
Social media
Economic indicator

ABSTRACT

Social media has been used as both a communication tool and a policy evaluation tool in the public sector. Moreover, it has gradually become an important source for big data analytics in policymaking. However, little academic research has focused on the socio-technical problems that stem from the use of social media as a source for big data analytics in the public sector. This paper sheds light on such problems by focusing on several economic development indicators from social media analytics in the Japanese government. The author analyses three types of challenges identified in previous literature on big data analytics: (1) governance and privacy, (2) organisational settings, and (3) quality and bias of the data. The analysis reveals that the Ministry of Economy, Trade and Industry (METI) has tackled the problems by (1) collecting data from a study group, (2) involving academically and/or industrially highly skilled professionals across the public and the private sectors, and (3) giving explanations for the developed indicator. This paper concludes with some recommendations for other governments.

1. Background/Literature Review

Big data has been regarded as the new 'oil' in the private sector (Bhageshpur, 2019). Recently, many enterprises have started to use social media not only as a communication tool but also as a data source for big data analytics in many business fields (He et al., 2013). In the public sector, however, the potential of social media as a data source has just started to be identified. This paper aims to discover socio-technical problems that arise when the public sector uses social media as a source of big data analytics in policymaking.

Social media has been primarily used by the public sector as a communication tool among citizens. Here, researchers have focused on its function to reflect public opinion and contribute to democratic processes. They have pointed out that social media does not sufficiently represent citizens due to the digital divide and increasing amount of fake information. Nevertheless, it supports the public sector to collect opinions in real time (Desouza & Jacob, 2017). Subsequently, social media has been used as a policy evaluation tool, with which the public sector can measure the effectiveness of services quantitatively. For instance, Agostino & Arnaboldi (2017) propose a way of measuring public service effectiveness using Twitter data.

However, there is little research on how the public sector can use social media as a source for big data analytics. Desouza & Jacob (2017) point out the potential of social media as a prediction tool in the policymaking process, but empirical analysis from a socio-technical perspective is still needed to reveal the challenges for such use in the public sector (Vydra & Klievink, 2019). Regarding big data analysis in general, many researchers have addressed socio-technical problems in the public sector. Three types of concerns have been identified in the past literature. First, privacy and security are critical due to the need to collaborate across multiple agencies (Desouza & Jacob, 2017; Höchtl et al., 2016; Pencheva et al., 2018). Second, organisational setup, including the lack of capabilities for data analytics, matters in the implementation (Höchtl et al., 2016; Pencheva et al., 2018). Third, data quality and bias might cause problems (Desouza & Jacob, 2017; Höchtl et al., 2016). These points might cause inappropriate and inefficient use of big data in the public sector, and whether these problems are common in social media use as a source of big data analytics in the public sector is the theme of this paper.

The author selected economic prediction in the public sector as an example of social media data analytics, because economic prediction is an influential policymaking field directly affecting national economic policy (Blazquez & Domenech, 2018). Some research has previously introduced the methodology from a technological forecasting perspective; for example, Indaco (2018) indicates that Twitter data may be used to measure country-level gross domestic

Corresponding Author
Email Address: idemitsu1101@gmail.com

product (GDP) in a more timely manner compared to conventional estimations.

In addition, according to some reports from practitioners, several governments have attempted to implement social media data analytics as a source of economic prediction. For example, the Australian government tries to extract skills and competencies data from LinkedIn to understand the dynamics of the labour market (World Bank, 2017). However, scant academic research analyses these items. Therefore, this paper addresses the socio-technical problems in sourcing social media data for big data analytics, using the example of economic prediction. The remainder of the paper consists of four sections. Section 2 introduces the research design, section 3 describes a use case, section 4 analyses the challenges, and the final section concludes this paper.

2. Research Design

The research question of this paper is: 'What are the socio-technical challenges in social media use as a source of big data analytics in the public sector?' In order to explore the question, this paper adopts a case study approach (Flick, 2014) which enables researchers to empirically investigate the details of a particular phenomenon (Yin, 2014). The author selected a case in the Japanese government, because it was one of the earliest attempts of developing new economic indicators based on social media data analysis.

The author collected data from open source documentation, such as official websites and government reports, and analysed the three socio-technical challenges raised in the literature, as explained previously (Desouza & Jacob, 2017; Höchtl et al., 2016; Pencheva et al., 2018).

3. Case Description

The Ministry of Economy, Trade and Industry (METI) in Japan has developed several economic indicators by utilising big data since 2014 (METI & PwC Aarata LLC, 2017). In 2016, METI conducted a project "to complement, expand, and refine existing government statistics, and to develop indicators that are more prompt and accurate than existing statistics" (METI & PwC Aarata LLC, 2017, p. 7). In particular, METI commissioned a private securities company to develop an index of economic situation as a demonstration project. At the same time, an expert study group was formed to accompany the development and utilisation of the indicators.

As a result of the project, METI and the agency developed a model to estimate the Index of Industrial Production (IIP) using metrics from Twitter and blogs. According to the report (METI & PwC Aarata LLC, 2017), they first selected about 200 keywords that were considered to be strongly related to the macro index. For instance, the word "overwork" was considered to be a keyword because it represents the increase of production in manufacturing. Then, they measured the correlation between the frequency of these words and the statistical index, such as IIP. Next, they analysed the text in the documents that contained those words and included only meaningful tweets (e.g. "I overworked today."), excluding unrelated ones (e.g. "I didn't overwork today."). The obtained values were used to create a time series model in order to compare with IIP (METI & PwC Aarata LLC, 2017, p. 40).

This analysis included two essential methods: text mining and sentiment analysis. Text mining is "the systematic analysis of large-scale text collections" (Grimmer & Stewart, 2013, p. 268). It usually employs the bag-of-words model (Zhang et al., 2010) to categorise words, pre-process the text and create a document-feature matrix, which represents the frequency of each word in the whole text. The second method, sentiment analysis, estimates people's sentiment from the text (Pang & Lee, 2008). Sentiment analysis is usually conducted by

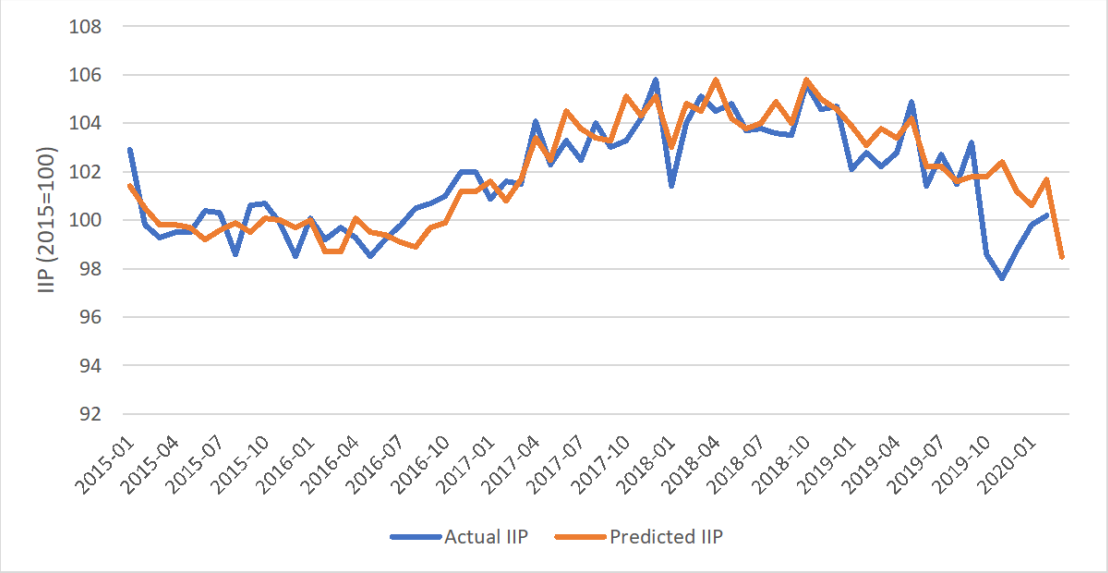


Figure 1. Comparison between actual IIP and predicted IIP (data source: METI (2020); Nomura Security Co., Ltd. (2020))

extracting the frequency of sentiment keywords (i.e. using a dictionary of sentiment keywords with the document-feature matrix made in the text mining). By combining these two methods, METI predicted real-time economic situations (see Figure 1).

METI concluded that metrics using Twitter and blogs were able to estimate the IIP with higher accuracy than those that did not use them. They emphasised the advantages, i.e. this estimation could be updated on a daily basis and could be used as a quick policy decision and investment indicator. Also, the accuracy is significantly higher than existing indices, which could improve the accuracy and speed of IIP predictions. On the other hand, METI pointed out that the model using only Twitter data was not accurate than that using multiple sources including blog data (METI & PwC Aarata LLC, 2017, p. 51).

4. Analysis

This paper analyses the case concerning the three challenges known from literature as explained in section 1: (1) governance and privacy, (2) organisational settings, and (3) data quality and bias.

First, the privacy issue is critical in social media data because the data is rarely anonymised. Further, the authors do not assume that their microblogs are mined by the public sector, although those microblogs are open to the public as long as the author does not opt out (Benedikt & Tew, 2019). Social media companies explicitly define usage rights for public entities in order to avoid inappropriate use. For instance, the Twitter Developer Agreement Policy prohibits the sharing of content with "Government End Users, whose primary function or mission includes conducting surveillance or gathering intelligence" (Twitter.com, 2020).

METI cleared this point by concluding a contract with the data collection companies. The companies formatted the raw data and passed it on to METI, which required those companies to follow the privacy rules in the contract. However, METI had to balance the conflicting goals of securing flexibility of data analysis, e.g. direct access for data source and data privacy. The company 'owning' the social media data conducted an analysis of social media indicators in the project, and denied raw data access due to security reasons (METI & PwC Aarata LLC, 2017; p. 233). This inflexibility is one of the limitations of social media analytics for public entities.

Second, social media analytics, like big data analytics in general, requires expertise. Academic research points out the lack of skills and human resources within the public sector. Therefore, METI partnered with several companies in the project. In its project report, METI indicates that the objective of the project was not only for the government to help making prompt and accurate economic and policy decisions, but also for the private sector to make quick and appropriate management decisions (METI & PwC Aarata LLC, 2017, p. 7). This second objective enabled METI to involve private sector companies in order to gain access to the expertise needed for social media analysis.

However, the project contract was limited to one year due to budget constraints. This meant that METI needed to renew the contract annually. Occasionally, an indicator is completely dependent on a company's technology. Thus, transferring the technology to the government may create a problem of intellectual property rights given that the indicator will be formally published in the following year or later. For instance, one METI indicator was dependent on a technique to extract target users from Twitter, which could only be performed by one special company. While the indicator was not used in the end, this problem would have occurred, if it had been applied as an official indicator.

Finally, quality and bias of data are problematic in social media analytics as well as in big data analytics in general. In terms of quality, METI mentioned in the report that "the model using only social media cannot be estimated with high accuracy; thus, we will consider combining multiple models to improve accuracy" (METI & PwC Aarata LLC, 2017, p. 51). Also, METI mentioned that there was missing data due to the error of social media data collection (ibid, p. 51). Further, as real-time tweets were collected via application programming interfaces (APIs) from Twitter, some data could not be verified later. The public sector needs to overcome this uncertainty by enhancing resilience of data collection, if they use social media data as an official statistic.

Moreover, a precise explanation is needed when the government releases the outcome of social media analytics. Although social media analysis can provide strong evidence of economic dynamism, governments tend to fail to provide in-depth reasons for policy choices, as some researchers pointed out in the research of evidence-based policymaking (De Marchi et al., 2016). Some biases are inevitable even if the developed indicator seems to represent the trend of markets, because social media users are not representative of the full population (Desouza & Jacob, 2017). For instance, there is a veracity issue in geolocation data on Twitter, since only ca. 20% of all tweets are tagged by geolocation data (Benedikt & Tew, 2019). Therefore, governments need to be cautious about reliability when they use indicators derived from social media data analysis.

5. Conclusion

This paper addressed the research gap and socio-technical problems of social media data mining and analysing in the public sector. It analysed a case of METI to show risks and opportunities. There are three lessons from METI's case for practitioners.

Firstly, governments need to consider privacy issues when they collect social media data. One possible solution is making a privacy contract with agency companies, as METI did in their project. METI evaluated alternatives of collecting data by establishing a study group. As such, governments will be required to consider possible choices and select the most appropriate way of data collection when they use social media data as a data source of big data analytics.

Secondly, sharing a common goal with partner companies and academic institutions is critical to complement necessary skills and knowledge for social media analysis. In general, the public sector has budgetary constraints on hiring highly skilled professionals, but METI became a platform to develop economic indicators by raising the common goal across the private sector. The example indicates the opportunities for governments to become a platform of big data analytics as well as social media analytics.

Finally, a clear explanation is necessary to build trust with citizens and businesses when the government delivers the project to the public. The developed indicators are open to the public in METI's official website with explanations about the accuracy and potential biases. Such explanations might be needed, if other governments release the results of social media analytics.

This paper concludes with limitations and the future research direction. First, the project was conducted in 2016 and 2017. Thus, further research is needed based on the recent development of technologies. Second, METI's project was outsourced to several companies. Hence, there might be different socio-technical problems in other forms of project management. Finally, the main source of social media data was Twitter. However, different social media might have different characteristics, which could cause distinct kind of socio-technical problems. Further research is needed from these points of view in the future.

References

Agostino, D., & Arnaboldi, M. (2017). Social media data used in the measurement of public services effectiveness: Empirical evidence from Twitter in higher education institutions. Public Policy and Administration, 32(4), 296–322. https://doi.org/10.1177/0952076716682369

Benedikt, L., & Tew, E. (2019, February 5). Can social media data improve official statistics? Not yet, suggests new work on tourism | National Statistical. https://blog.ons.gov.uk/2019/02/05/can-social-media-data-improve-official-statistics-not-yet-suggests-new-work-on-tourism/

Bhageshpur, K. (2019, November 15). Council Post: Data Is The New Oil -- And That's A Good Thing. Forbes. https://www.forbes.com/sites/forbestechcouncil/2019/11/15/data-is-the-new-oil-and-thats-a-good-thing/

Blazquez, D., & Domenech, J. (2018). Big Data sources and methods for social and economic analyses. Technological Forecasting and Social Change, 130, 99–113. https://doi.org/10.1016/j.techfore.2017.07.027

De Marchi, G., Lucertini, G., & Tsoukiàs, A. (2016). From evidence-based policy making to policy analytics. Annals of Operations Research, 236(1), 15–38. https://doi.org/10.1007/s10479-014-1578-6

Desouza, K. C., & Jacob, B. (2017). Big Data in the Public Sector: Lessons for Practitioners and Scholars. Administration & Society, 49(7), 1043–1064. https://doi.org/10.1177/0095399714555751

Flick, U. (2014). An introduction to qualitative research (5th ed.). Sage Publications.

Grimmer, J., & Stewart, B. M. (2013). Text as Data: The Promise and Pitfalls of Automatic Content Analysis Methods for Political Texts. Political Analysis, 21(3), 267–297. https://doi.org/10.1093/pan/mps028

He, W., Zha, S., & Li, L. (2013). Social media competitive analysis and text mining: A case study in the pizza industry. International Journal of Information Management, 33(3), 464–472. https://doi.org/10.1016/j.ijinfomgt.2013.01.001

Höchtl, J., Parycek, P., & Schöllhammer, R. (2016). Big data in the policy cycle: Policy decision making in the digital era. Journal of Organizational Computing and Electronic Commerce, 26(1–2), 147–169. https://doi.org/10.1080/10919392.2015.1125187

Indaco, A. (2018, July 12). From Twitter to GDP: Estimating Economic Activity From Social Media. Proceedings of the 2nd International Conference on Advanced Research Methods and Analytics (CARMA 2018). CARMA 2018 - 2nd International Conference on Advanced Research Methods and Analytics. https://doi.org/10.4995/CARMA2018.2018.8316

METI. (2020, March 31). Index of Industrial Production (production / shipment / inventory, production capacity / occupancy rate), manufacturing industry production forecast index (鉱工業指数(生産・出荷・在庫、生産能力・稼働率)、製造工業生産予測指数). https://www.meti.go.jp/statistics/tyo/iip/result-1.html

METI, & PwC Aarata LLC. (2017). 平成28年度 IoT推進のための新産業モデル創出基盤整備事業 （ビッグデータを活用した新指標開発事業） 報告書 (FY2016 New Industrial Model Creation

Infrastructure Development Project for Promoting IoT (New Index Development Project Utilizing Big Data) Report).

Nomura Security Co., Ltd. (2020, March 31). SNS×AI IIP prediction index (SNS×AI 鉱工業生産予測指数). http://qr.nomura.co.jp/quants/sns_ai/#jump4

Pang, B., & Lee, L. (2008). Opinion mining and sentiment analysis. now Publishers Inc.

Pencheva, I., Esteve, M., & Mikhaylov, S. J. (2018). Big Data and AI – A transformational shift for government: So, what next for research? Public Policy and Administration, 095207671878053. https://doi.org/10.1177/0952076718780537

Twitter.com. (2020, March 10). Developer Agreement and Policy – Twitter Developers. https://developer.twitter.com/en/developer-terms/agreement-and-policy

Vydra, S., & Klievink, B. (2019). Techno-optimism and policy-pessimism in the public sector big data debate. Government Information Quarterly, 36(4), 101383. https://doi.org/10.1016/j.giq.2019.05.010

World Bank. (2017). Big Data in Action for Government: Big Data Innovation in Public Services, Policy and Engagement (English). World Bank Group. http://documents.worldbank.org/curated/en/176511491287380986/Big-data-in-action-for-government-big-data-innovation-in-public-services-policy-and-engagement

Yin, R. K. (2014). Case study research: Design and methods (Fifth edition). SAGE.

Zhang, Y., Jin, R., & Zhou, Z.-H. (2010). Understanding bag-of-words model: A statistical framework. International Journal of Machine Learning and Cybernetics, 1(1–4), 43–52. https://doi.org/10.1007/s13042-010-0001-0

iS
CHANNEL

How Big Data Impacts Research and Knowledge Generation: An Epistemological View

Yiduo Wang

MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Literature Review
Big Data
Epistemology
Knowledge Generation
Prediction
Research
Social Sciences

ABSTRACT

Big data is a prevalent topic in today's news and articles, along with the opportunities it has created for academic research and business activities. However, it is difficult to analyse the real impact without an understanding of how big data has changed the way we generate knowledge. Therefore this review adopts an epistemological view. It critically engages with the literature and summarises two dominating themes. First, big data enables a new way of proposing theories by recognizing patterns purely from data. Second, the expansiveness of big data empowers large scale predictions in many areas. This review juxtaposes assumptions both for and against each argument and concludes that while big data has indeed created new disciplines and research paradigms, it is not a panacea for all the problems. Rather, asking the right questions and employing the appropriate methods are still critical to scientific discovery and value creation. Regarding literature selection, the author started from several Information Systems and Media and Communication journal articles and looked at their references for relevant literature, particularly those with keywords "big data", "epistemology", "theory" and "prediction". A group of articles are critically selected to give a comprehensive overview of the topic.

Introduction

The rise of big data has been much heralded in recent years, in company with technological progress such as increased computing power and the Internet of Things (IoT). Big data is not simply a technological advancement but has revolutionized business activities, academic research, human relationships and social interactions - namely every aspect of society. This critical literature review focuses on the epistemological discussions of big data. Epistemology, which originates from the Greek word epistēmē meaning "knowledge", is defined as "the study or a theory of the nature and grounds of knowledge especially with reference to its limits and validity" (Merriam-Webster's dictionary, n.d.). Therefore, the following review highlights how big data has changed the way academics and business generate knowledge as well as the validity of methodology used for big data analysis.

This article is structured as follows: first, big data is defined, with reasons why it differs from "small" data and accounts for a new epistemological change. Then, two categorizations from the literature are identified and introduced: one is the changing format of theory generation, the other is the unprecedented predictive power big data has created. Within both themes, views from proponents and detractors are carefully reviewed and validated with examples from various disciplines. Finally, this review ends with concluding remarks and possible areas for improvement and future research.

Defining Big Data: A Historical Review on Epistemology Changes

There are different views regarding how big data is defined. One school looks at big data comprehensively, identifying the scope and boundaries of big data from different perspectives. Ekbia et al. (2015) identified four main perspectives in the existing literature. The first perspective is product-oriented with a focus on the attributes of data, such as massiveness in volume, and data format such as audio or video. This perspective is adopted by Baesens et al. (2016) who defined the five "V" s of big data: volume, velocity, variety, veracity and value. The second perspective is process-oriented and underscores the novelty of processes that are required to analyse big data. For instance, the requisite technological infrastructure, tools and programming techniques advance with the emergence of both structured and unstructured data in various forms, such as text, audio, video and clickstream. The third perspective is cognition-oriented and highlights the concern that the human mind is no longer able to make sense of the large amount of data. This includes "capacity to search, aggregate, and cross-reference large data sets" (Boyd and Crawford, 2012, p.665). Finally, the fourth perspective, which was not explicitly mentioned in previous literature,

Corresponding Author
Email Address: yiduowang1234@outlook.com

is the social movement perspective. The emphasis is the socio-technical impact technology (big data) has on wider society, including economics, politics and culture. This view sees big data technologies as developed within a complex ecosystem formed by technology companies, the open source community, governments, and universities. For example, Yahoo! Supported the development of Apache Hadoop, the widely adopted open source framework in big data research, and IBM collaborated with universities to set up Data Science and Business Analytics programmes (Ekbia et al., 2015).

Other authors focus on the more distinctive feature of big data and argued that largeness in terms of size is not the main development (Chandler, 2015; Mills, 2018). Historically, there have been datasets larger than those currently regarded as big data, such as census data (Boyd and Crawford, 2012) and diary studies. One example, reported by Mills (2018), is the International Time-Use Study of 1965 by Szalai (1972), with 2,000 interviewees, aged 18-64 from 12 countries. Big data only renders the manual recording method obsolete but has no significant change in terms of data volume or time span. Rather, the distinction is that big data is not collected by researchers or governments to test a theory or validate a hypothesis, but is automatically generated from social media, mobile technologies, IoT, and on the internet. Therefore, data analysts seek to gain insights from data that already exists (Chandler, 2015). Such a view introduces the first theme of this literature review.

Regarding the changes big data creates, two themes dominate. One is that the vast amount of data provides an agnostic and comprehensive source of evidence, and therefore may change the way theories are proposed, tested and validated. This shift calls into question the correlation and causation between variables, which introduces a second topic regarding the predictive power of big data. That is, data reveals insights and predicts future trends even when the underlying mechanism is not clearly understood. Of course, both suffer from flaws, and these will be discussed in greater detail in the rest of this paper.

New Forms of Inquiry: "Data Speaks for Itself"

The vast amount of complex and relational datasets coupled with data analytics' techniques have challenged epistemologies in disciplines across the sciences, social sciences and humanities (Kitchin, 2014). Instead of collecting appropriate data for the sake of validating hypotheses and theories, researchers use data generated automatically from everyday behaviour. With the same input datasets, decisions such as which variables to count, which data to clean and what algorithms and models to employ lead to different results which sometimes engender unexpected discoveries (Dhar, 2013; Ekbia et al., 2015). Consequently, the computer is no longer "a pure analytic servant" but "an active question asking machine" (Agarwal and Dhar, 2014, p.444). Kitchin (2014) described this as a "new forms of empiricism" (p.1); that is, an epistemological approach for making sense of the world that is enabled by big data analysis. Rather than testing a theory by gathering relevant data, insights are acquired "born from the data" (ibid., p.2).

This shift in research paradigms is seen as a huge opportunity, or even a complete epistemic change towards an empiricism in which knowledge and patterns emerge from data themselves. One provocative forecast is voiced by Anderson (2008), stating that the scientific method of "hypothesize, model, test" is obsolete due to the deluge of data. He validated his argument by using the example of Craig Venter, who discovered thousands of previously unknown species of bacteria and other life-forms by statistically analysing and comparing large amounts of gene sequence data detected in the ocean and air, without knowing much of the new species. Such views are criticized fiercely by Pigliucci (2009), a philosopher of science, claiming that Anderson (2008) does not understand science and scientific methods. Although finding patterns is part of the scientific method, science is more about explanations for those patterns. Therefore, Venter's finding is just a starting point to form hypotheses. Without hypotheses to be tested, the data are just a "useless curiosity" (Pigliucci 2009, p.534). Even in a business scenario, advertisers are interested in theories of human behaviour and those theories act as guidance when making decisions about which data are collected and which keywords are used to organise the search. Moreover, Kitchin (2014) and Lazer et al. (2014) argue that the ability to recognise patterns also stems from previous scientific discoveries when theories are tested for validity and veracity. Thus, big data does not come out of a scientific vacuum but are part of a cumulative endeavour.

Besides the above debate regarding whether data is generated free from theory, the efficacy of such an inductive and empiricist scientific discovery approach pre-assumes some ideas underpinning its formulation, which could be fallacious (Kitchin, 2014). Two assumptions are summarized in the literature.

First, big data seeks to be exhaustive so that full resolution of the worldwide affairs can be captured (Steadman, 2013). However, data represents only parts of the population. For example, Boyd and Crawford (2012) pointed out that "people" and "Twitter users" are not synonymous and Twitter does not represent "all people" (p.669). Similarly, Floridi (2012) argued that the real epistemological problem with big data is the "small patterns" generated from pieces of data (p.436). Given that so much data can now be generated and processed so quickly and cheaply and on virtually anything, the pressure is to identify real value-adding patterns from the immense database. Such patterns, if found, only represent parts of the truth and would only be significant if aggregated properly. The requirement of aggregation and sense-making introduces the difficulty of integrating multiple data sources, both due to the constraints of computational power and the need to spot what has value in the data noise.

This leads to the second assumption that with big data, context or domain-specific knowledge is no longer needed, or is needed very little, in order to interpret

the data statistically (Anderson, 2008; Steadman, 2013). In order to recognize value from data noise, Floridi (2012) argues, techniques and technologies do help but are insufficient. Some data and computer scientists are active in practicing social science research are prone to "big data hubris" (Lazer et al., 2014, p.1203). Kitchin (2014) cites an example when a group of physicists employed big data analytics to model social and spatial processes in cities, hence suggested laws underpinning the process of city formation. He was critical that such studies often ignore both century-long social science practice and the effect of culture, politics and capital. From this point of view, it seems that the epistemological impact of big data is not fundamentally different to other new technologies which have changed measurement in scientific research (Kitchin 2014). The persistent problems remain; as Floridi (2012) quoted Plato (Cratylus, 390c), the crucial problem is "know how to ask and answer questions".

Predict from Big data: Casual Relations versus Statistical Correlations

Data-intensive disciplines and corresponding techniques can be traced backed to the 18th century with the development of statistics. There have long been debates about the difference between correlation and causal relationships, albeit less intensively, between the proponents of data-driven science and those of theory-driven science (Hey et al, 2009, cited by Ekbia et al. 2015). The same discourse continues to the big data age, when the deluge of economic and social transactions online make data much easier to access and make it easier to discover correlations among variables. The strain between correlational analysis and causal testing of hypotheses introduces the differences in the explanatory versus predictive power of big data. As has been argued by the philosopher of science Karl Popper, "prediction is a key epistemic criterion for assessing how seriously we should entertain a theory of a new insight: a good theory makes bold predictions that stand repeated effects as falsification." (Popper 1963, cited by Agarwal and Dhar (2014). Therefore, predictive power could be one of the strengths of big data.

However, some examples in the literature revealed different stories. Prediction using large-scale online data faces inherent difficulties when it goes beyond describing phenomena and tries to generalize public behaviour. For instance, Ekbia et al. (2015) reported the Emotive project where British researchers used Twitter and other social media data to map the emotions of the nation. Two thousand tweets were analysed per second and each tweet was categorised into eight human emotions (anger, disgust, fear, happiness, sadness, surprise, shame, and confusion). The researchers claimed their results could "help calm civil unrest and identify early threats to public safety" (BBC, 2013, para. 3). Nevertheless, Ekbia et al. (2015) questioned the validity of this prediction in two aspects. Socially, it is unclear to what extent this 'threat identification' is valuable for law reinforcement and under what context this will lead to order rather than chaos. Technically, two assumptions restrict the veracity of the result. First, human emotions can be reduced meaningfully to only eight categories, ignoring more subtle ones such as grief and contentment. Second, within the same category, emotions are expressed broadly without a distinction between, for example, happiness in different situations. Accordingly, these limitations may erode the credibility of the proposed prediction system.

More examples seem to support this view and raise concern over prediction using big data. Lazer et al. (2014) used the Google Flu Trends (GFT) example when Google tried to predict the number of doctor visits for influenza-like illnesses by key-word searching from 2009 to 2014. Even with improved models, the prediction is still two times higher than the actual record from Centers for Disease Control and Prevention (CDC) (Lazer et al., 2014). They analysed the causes for this deviated prediction and concluded with two reasons, namely "big data hubris" (Lazer et al., 2014, p.1203) and "algorithm dynamics (ibid., p.1203)". The assumption of the former is that big data are not a supplement to, but substitute for, traditional data aggregation and evaluation. This is a common hypothesis seen in big data related literature (Chandler, 2015; Dhar, 2013) and originates from the conceit of data and computer scientists who may practice social science without certain domain knowledge (Ekbia et al., 2015), as discussed before.

Therefore, the author calls for an "all data revolution" rather than a "big data revolution" (Lazer et al., 2014, p.1203) which emphasizes a combination of the traditional statistical methods with the new big data methodology. "Algorithm dynamics" (ibid., p.1203) mean that the algorithms alter in accordance with the business model of the commercial companies. That is, during the time span of the GFT project, Google also changed the data generating process (its algorithm) to improve customer service. While GFT takes in the assumption that the search frequency for certain terms is related to, and can reflect, external events, search behaviour was co-determined by exogenous determinants (such as user behaviour) as well as endogenous mechanisms (such as different algorithm models). "Algorithm dynamics" (ibid., p.1203) are also seen in other platforms such as Twitter and Facebook; since service providers kept re-engineering the algorithm, it was almost impossible to replicate the results. This poses an open question on the duplication ability of such big data research (Lazer et al., 2014) and contradicts with Kitchin (2014)'s proposition that the extensiveness of data makes it easier to test the veracity of theories.

The above two examples show what happens when the purpose of data-generating and data-analysing organizations (such as Twitter, Google and Facebook who emphasise profit and revenue) does not align with the purpose of what they are predicting (usually public affairs with the intention to enhance social welfare). Nevertheless, in business areas, big data prediction is valuable in terms of revenue generation and customer retention. Baesens et al. (2016) introduced several business use cases in their article, and one example was to use behaviour data to improve targeted marketing. Fine-grained transaction

data were analysed to predict which financial products individual customers were most likely to buy, and the results were not only of great value but also had higher quality with bigger data. The above instances highlight the urgency of selecting big data methods in the appropriate context. In short, big data is a powerful tool and can indeed provide insights in some circumstances, but the predictive power of big data again depends highly on what questions are asked and what context is studied.

Concluding Remarks

To conclude, this article recognized two distinctive features of big data, namely a new way of generating theories and the power to predict numerically from models and algorithms. Thus, it is pivotal to understand the question being asked so that appropriate data sets can be used to draw conclusions and insights.

This critical literature review could be further improved in terms of depth and breadth. It focused on a contemporary topic, in which most referenced articles are concentrated in the last decade. As there have been several shifts in research paradigms, it is worth putting big data into a historical context and comparing it with other scientific milestones such as the big science era after World War II. Also, for each of the two topics discussed, there are books worth looking at which would add more perspectives to the debate. For instance, Raw Data Is an Oxymoron questions the claims made about the objectivity of big data, and The Signal and the Noise: Why So Many Predictions Fail – but Some Don't would serve as good complementary reading for the prediction discourse. For breath, a third topic regarding big data and qualitative research is mentioned repeatedly in the literature but not elaborated on in the main text of this critical literature review due to time and word limits. Briefly, the massive amount of easily accessible data has also captured the imagination of qualitative researchers and several pieces of literature have mentioned the threats to, and potential of, big data in qualitative research (Ekbia et al. 2015, Mills 2018, Parks 2014). Interdisciplinary studies, such as computational social science and digital humanities, are also being developed due to big data, and would generate interesting discussion.

References

Anderson, C., 2008. The end of theory: The data deluge makes the scientific method obsolete. Wired, [online] 23 June 2008. Available at: http://www.wired.com/science/discoveries/magazine/16-07/pb_theory (accessed 06 December 2019).

Agarwal, R., & Dhar, V. (2014). Editorial —Big Data, Data Science, and Analytics: The Opportunity and Challenge for IS Research. Information Systems Research, 25, 443–448. https://doi.org/10.1287/isre.2014.0546

Baesens, B., Bapna, R., Marsden, J. R., Vanthienen, J., & Zhao, J. L. (2016). Transformational Issues of Big Data and Analytics in Networked Business. MIS Quarterly., 40(4), 807–818. https://doi.org/10.25300/MISQ/2016/40:4.03

BBC, 2013. Computer program uses Twitter to 'map mood of nation'. BBC, [online] 7 September 2013. Available at: http://www.bbc.co.uk/news/technology-24001692 (accessed 13 December 2019).

Boyd, Danah, & Crawford, K. (2012). Critical Questions for Big Data. Information, Communication & Society, 15(5), 662–679. https://doi.org/10.1080/1369118X.2012.678878

Chandler, D. (2015). A World without Causation: Big Data and the Coming of Age of Posthumanism, Millennium, 43(3), 833-851. https://doi.org/10.1177/0305829815576817

Dhar, V. (2013). Data Science and Prediction. Communication ACM, 56(12), 64–73. https://doi.org/10.1145/2500499

Ekbia, H., Mattioli, M., Kouper, I., Arave, G., Ghazi, A., Bowman, T., Sugimoto, C. (2015). Big Data, Bigger Dilemmas: A Critical Review. Journal of the Association for Information Science and Technology, 66(8). 1523-1545. https://doi.org/10.1002/asi.23294

Epistemology. (n.d.) In Merriam-Webster's dictionary. Retrieved from https://www.merriam-webster.com/dictionary/epistemology

Floridi, L. (2012). Big Data and Their Epistemological Challenge. Philosophy & Technology, 25(4), 435–437. https://doi.org/10.1007/s13347-012-0093-4

Kitchin, R. (2014). Big Data, new epistemologies and paradigm shifts. Big Data & Society, 1(1), 2053951714528481. https://doi.org/10.1177/2053951714528481

Lazer, D., Kennedy, R., King, G., & Vespignani, A. (2014). The Parable of Google Flu: Traps in Big Data Analysis. Science, 343(6176), 1203–1205. https://doi.org/10.1126/science.1248506

Mills, K. A. (2018). What are the threats and potentials of big data for qualitative research? Qualitative Research, 18(6), 591–603. https://doi.org/10.1177/1468794117743465

Parks, M. R. (2014). Big Data in Communication Research: Its Contents and Discontents. Journal of Communication, 64(2), 355–360. https://doi.org/10.1111/jcom.12090

Pigliucci, M. (2009). The end of theory in science? EMBO Reports, 10(6), 534. https://doi.org/10.1038/embor.2009.111

Steadman, I., 2013. Big data and the death of the theorist. Wired, [online] 25 January 2013. Available at: http://www.wired.co.uk/news/archive/2013-01/25/big-data-end-of-theory (accessed 10 December 2019).

iS
CHANNEL

Perspectives on Business and Technology Alignment

Jiao (Joanna) Peng

MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

Business and technology alignment
Strategy
Strategizing
Planning

ABSTRACT

The alignment between business and technology is considered important to the business. Yet, there is little agreement on how alignment can be managed in an organisation. There are two streams of opinions: alignment can be rationally planned and controlled; or alignment is fuzzy, improvised and cannot be entirely predicted. The differences between the perspectives result in different recommendations and observations from research. Literature based on the former perspective usually attempts to identify good alignment practices. It also emphasises the importance of good upfront planning. On the other hand, literature based on the latter perspective typically reflects on how alignment occurs and how to respond to unintended changes. Furthermore, with the pervasive use of digital technology in recent years, both streams of literature recognise the dynamism of technology. The view that alignment is an ongoing process has become more popular. Thus, it is essential to embed flexibility and adaptability in an organisation's strategic planning, structural design and operation.

1. Introduction

The alignment between technology and business has been researched for over three decades. It is also reported as a top concern for management and IT practitioners (Luftman et al., 2017). Then, what is alignment? Emergent from the search for strategic business and IT planning and IT-led organisational transformation techniques in the 1980s, alignment broadly refers to where an organisation uses technology appropriately given their situations, business needs and goals (Coltman et al., 2015; Luftman, 2000). Various terms have been used to express alignment, including 'linkage' (Henderson & Venkatraman, 1993), 'fusion' (Smaczny, 2001) and 'bridge' (Ciborra, 1997). The use of different terms indicates that there are different perspectives on how alignment can be pursued.

This essay reviews how alignment takes place in an organisation, how it can be managed, and what the different perspectives on this topic are. The differences between the perspectives influence the observations and recommendations from the research. There are two different streams of opinions: alignment can be rationally planned and controlled; or it is fuzzy, improvised and cannot be entirely predicted. Additionally, as technology develops over time, especially with the pervasive use of digital technology in recent years, the first stream can be further divided based on whether it views IT and business as distinctly separate or integrated. The view on alignment itself has also evolved from being a state or an outcome to being broadly recognised as an ongoing process.

To view the different perspectives, research papers were selected mostly from top tier IS journals. Additionally, only papers with the main topic on alignment were selected. In order to understand how the research has evolved, both classical papers and recent research were included.

This paper is structured as follow. First, I discuss the different perspectives on alignment based on their underlying assumptions. I then discuss the connections between different perspectives, limitations and possible future research.

2. Different Perspectives on Business and Technology Alignment

2.1 Alignment can be rationally planned and controlled

The most common underlying assumption in the alignment literature is that alignment can be rationally planned and controlled. Recognising it is a complex organisational issue that management is highly interested in, many researchers have been working on providing guidance on how to manage better and achieve alignment. This research can be further categorised into two groups based on whether technology and business are viewed separately or at different levels.

2.1.1 Business and technology are distinctly separate

The needs of alignment initially emergent from acknowledging technology are vital in helping business perform well, and technology and business are structurally separate. There is a large variety of

Corresponding Author
Email Address: joannapeng@hotmail.com

research available in this category. One of the best-known models is the Strategic Alignment Model (SAM) by Henderson and Venkatraman (1993). According to SAM, there are four domains which require alignment: business strategy, IT strategy, business infrastructure and IT infrastructure. All four domains are cross related, and alignment is required for strategy, infrastructure and structure. SAM also recognises the importance of the relationship and interactions between business and technology and seeing alignment as making choices at each domain (Luftman et al., 2017; Peppard & Breu, 2003).

SAM was considered a radical idea at the time (Coltman et al., 2015). It inspired people to move away from planning IT investments and operations in isolation and thinking about their linkage with business strategy (Coltman et al., 2015). It also considers alignment not only required at the strategy level but also at the operation level (Chan & Reich, 2007). However, SAM is a conceptual model with four static components. Therefore, it does not provide sufficient insights into how alignments are achieved (Coltman et al., 2015; Luftman et al., 2017). This has motivated further research conducted in this area. One example is Luftman's series of papers on alignment enablers, inhibitors and maturity assessment (Luftman, 1996, 2000; Luftman et al., 2017). In their most recent Strategic Alignment Maturity assessment research, Luftman et al. (2017) view alignment as a series of activities carried out by IT and business jointly. The authors identify how activities from six categories: communications, value analytics, IT governance, partnering, dynamic IT scope and business and IT skills development, can impact alignment. A successful alignment requires business and IT teams to consider all these six categories together.

It is worthwhile noting that alignment research is not limited to models and key success factors. There is also research focusing on how the choice of stakeholders, their degree of involvement, and methods of communication and decision making influence alignment (Karpovsky & Galliers, 2015). Reich and Benbasat (2000) found that a shared understanding between business and technology can influence both long term and short term alignment. Additionally, IT implementation success, communication between business and technology executives, and connections between business and IT planning impact alignment on a short-term basis. Schlosser et al.'s (2015) research revealed similar findings – the shared understanding between business and technology could influence alignment positively. Their research also found that informal governance mechanisms, such as cross-functional events and cooperative activities, are more powerful in facilitating tactic knowledge sharing and developing better shared understanding.

2.1.2 Technology is embedded in business.

Despite suggesting IT can enable business, SAM views IT strategy as a functional level strategy and implies that business comes first, and technology needs to fit with business' needs (Bharadwaj et al., 2013; Smaczny, 2001). This view has been critiqued for its appropriateness, given the speed and scale of technology development and usage in recent years (Bharadwaj et al., 2013). Smaczny (2001) also argues that one of the key drawbacks of the 'fit' view is the synchronisation required between business and IT takes time. Consequently, organisations may not be able to respond to changes rapidly. Additionally, the 'IT follows business' approach could result in business missing out on business opportunities that are inspired or enabled by technology (Bharadwaj et al., 2013; Smaczny, 2001).

Smaczny (2001) proposes the fusion view of business and technology. In other words, there is only one strategy that covers both business and technology, and only one set of operation plans. It is not about 'aligning' technology and business, but how to use technology strategically to enable and support the generation of business benefits. This view has attracted more attention in recent years as the use of digital technology arises. Digital technology is observed as integrated and pervasive in business (Bharadwaj et al., 2013). Additionally, it can shape business by bringing new and different ways to create and capture business value (Bharadwaj et al., 2013; Hess et al., 2016; Sebastian et al., 2017). To truly leverage the power of digital technology, Bhardwaj et al. (2013) suggest considering business and technology at an equal level and having a 'Digital Business Strategy' that integrates business and IT strategy. The authors call for a move beyond alignment, and deliberately think about the differential business values and competitive advantages that technologies can unlock.

In response to the needs of developing Digital Business Strategy, some scholars have suggested conceptual building blocks that management can follow. Sebastian et al. (2017) recommend that management focuses on either responding to or anticipating customers' needs. In order to achieve the chosen strategy, the business should have a robust technology operation infrastructure and a flexible digital platform that allows them to experiment. Furthermore, once the strategic focus is chosen, management should not change it in order to stay focused. Similarly, Hess et al. (2016) also emphasise the importance of creating a plan that can navigate firms through complexity and ambiguity. They proposed to develop such a plan by putting business' strategic goals at the centre, assessing possible use of technology, changes in business model and structure, and evaluating financial constraints. While both acknowledge the dynamic and emergent nature of digital technology and recognise that technology can drive business changes, they are not fundamentally different from the core concept of SAM. They both view strategy as a pre-determined plan that needs to be set up-front to lead business direction, then makes adjustments at the infrastructure and operational levels to support the execution of the strategy. However, given the high level of dynamism, the business could find it is challenging to define a rigid strategic plan upfront (Yeow et al., 2018).

Because technology is continuously evolving and the business environment is highly dynamic, instead of focusing on how to achieve an aligned state, some

research suggests studying the aligning process and activities (Karpovsky & Galliers, 2015; Peppard et al., 2014). This school of research views alignment or fusion of business and technology as an interactive and ongoing process. It is usually differentiated from the other types of study by using the term "strategising" or "aligning". One of the example studies is Yeow, Soh and Hansen's (2018) research based on the dynamic capabilities theory. Dynamic capabilities refer to a company's ability to adjust and develop its resources and competences according to the environment in order to stay competitive (Yeow et al., 2018). Throughout the aligning journey, tensions are likely to arise from misalignment between resources and strategy. Organisations can take rational actions to resolve misalignment and tension, but these actions can trigger new tensions. For example, tension could occur when the existing business and IT resources do not meet the needs of newly emergent business needs; the aligning actions that reconfigure resources could resolve this tension but also create a new and unintended tension as they enlarge the gap between the enhanced or new resources and not-yet adapted strategy. The research highlights the complexity and dynamism of aligning and suggests a completely aligned state may not be possible to achieve. Therefore, it is more critical that enterprises stay adaptive and are able to manage both planned changes and emergent issues during the aligning process.

2.1.3 Section Summary

In summary, as a managerial topic, there is a large amount of literature that builds on the assumption that alignment can be rationally planned and controlled. The literature used to be dominated by the view that business and technology are distinctly separate, and technology needs to fit with business needs. In recent years, as the use of technology has become more pervasive, there is a rise of literature seeing business and technology as integrated. Common alignment guidance from both views is determining a strategic plan first, then adjusting the infrastructure and operations accordingly to support the implementation of the plan. However, guidance from the view that business and technology are integrated tends to place more emphasis on dynamism and recommends enterprises to consider this in their strategies, structures and resource designs, and operations.

2.2 Alignment is fuzzy and cannot be predicted

An alternative view is the relationships between technology and business are fuzzy and cannot be entirely controlled or predicted (Ciborra, 1997). Researchers who adopt this school of view see alignment as a dynamic, adaptive, multi-faceted process with an emphasis on its improvisation and unpredictability (Benbya & McKelvey, 2006; Chanias et al., 2019; Vessey & Ward, 2013). Researchers usually describe it as non-deterministic, non-linear relationship, and self-organised (Benbya & McKelvey, 2006; Peppard & Breu, 2003; Vessey & Ward, 2013). Additionally, recognising alignment is a social process, researchers believe study alignment in context is essential, as it enriches the understanding of how and why it occurs (Benbya & McKelvey, 2006; Ciborra, 1997; Vessey & Ward, 2013). It is worth mentioning that despite this view has been around since the 1990s, it is not as prevalent as the first stream that considers alignment as rationally plannable and controllable (Peppard et al., 2014).

The fundamental belief that alignment is unpredictable and improvised has several implications. One of them is seeing strategy and its role differently. Instead of seeing strategy as a detailed plan created by an one-off top-down process upfront, researchers see it as an ongoing adaptive activity that evolves from interactions between learning and doing, between top-down planning and bottom-up emergent activities (Chanias et al., 2019; Marabelli & Galliers, 2017; Vessey & Ward, 2013). Chanias et al.'s (2019) study of a European financial service's digital transformation journey is a good reflection of this view. In the case, management acknowledged they did not know what they could eventually achieve at the beginning. Instead of focusing on detailed analysis and planning upfront, they deliberately used a high-level strategy to set off the direction and allowed teams to explore and experiment, then continually developing and adapting the strategy based on the learning. Although strategy is still seen as important and necessary, it plays a much less deterministic role.

Another key reflection derived from seeing alignment as improvised and unpredictable is the need for balancing flexibility and control (Benbya & McKelvey, 2006; Chanias et al., 2019; Vessey & Ward, 2013). This has different implications for different organisational components and organisation levels. For example, for business and IS resources allocation, management should consider the balance between exploitation and exploration resources in order to explore while maintaining a degree of stability (Vessey & Ward, 2013). For IS infrastructure, organisations may want to take advantage of modular IS design to enable a fast IS infrastructure adaptation (Benbya & McKelvey, 2006). For governance, while business should support explorations and empower those involved in making decisions, these activities and decisions should still be subject to certain formal governance and monitoring systems, such as steering committees to ensure appropriate controls can evolve simultaneously and clear roles and responsibilities remain (Vessey & Ward, 2013). Because of the characteristics of non-linear relationships and unpredictability, having a good degree of flexibility while maintaining control could help enterprise adapt rapidly when new challenges and opportunities are observed.

Similar to the other stream of literature, most research from this stream is conducted at an organisation level. There is little research focus on the individuals involved in aligning activities, and how their day-to-day practices influence the alignment (Karpovsky & Galliers, 2015). In the limited literature I could locate, Marabelli and Galliers (2017) studied power and its influences in strategising. They noted that different forms of power co-exist and they do not occur in sequence; instead, they "co-mangle" (Marabelli & Galliers, 2017, p.359). Hierarchical power is good

at starting an initiative and can be used to promote empowering, and performative power is essential in keeping alignment sustainable. Thus, enterprises should consider utilising both.

In summary, studies build on the belief that alignment is a dynamic process with improvisation and unpredictability believe it cannot be entirely planned and controlled. Instead of developing a detailed strategic plan up-front and using it to manage alignment, it is more important to support business, technology, and their alignment to evolve over time. Enterprises need to have both flexibility and control in order to explore and adapt while remaining stable. Additionally, Enterprises should consider utilising different forms of power that co-exist and influence alignment differently.

3. Conclusion

In this literature review, different perspectives on business and technology alignment were reviewed. The different motivations behind the research influence the focus of the research. The stream of literature that builds on the assumption that alignment can be rationally planned and controlled focuses on identifying good practices, tools, and frameworks to manage alignment better. On the other hand, the research that believes alignment is improvised and cannot be entirely predicted and controlled focuses on gaining a deeper understanding of how and why it occurs. Both streams of literature reviewed in this paper are important to understand and manage business and technology alignment.

Although developed on different assumptions, there are similar findings from both streams of researches, especially in recent years. For example, both streams of research noted alignment is highly dynamic, and there is an increased number of researchers who suggest seeing it as an ongoing process instead of a one-off event. As a result, enterprises need to be able to adapt to changes quickly, and their structural designs also need to support the desires of exploring and experimenting. Furthermore, research from both streams considers not only tools and methods, but also the human actors involved in the process and their activities' influences on alignment. For instance, shared understanding and communication between business and technology. The biggest critique of the literature developed on the assumption that alignment can be planned and controlled is that it oversimplifies the complex real world, and it is a challenge to unpack and implement the guidance in reality (Ciborra, 1997). Luftman (2017) also commented that one of the limitations of his own research was lack of consideration of environmental, political and cognitive factors. Omitting these factors could result in incomplete guidances. On the other hand, the literature developed based on the assumption that alignment is improvised and cannot be entirely controlled usually considers the alignment context; however, context vary, and this needs to be taken into account when applying the reflections.

Moreover, although a variety of research is in place, there are still areas that could be studied further. Most alignment research is conducted at the organisation level (Karpovsky & Galliers, 2015). Vessey and Ward (2013) see alignment as an organisational activity that requires changes beyond the individual level. However, there is value in understanding individuals' engagement in alignment in detail, as alignment is unfolded through their day-to-day practice (Karpovsky & Galliers, 2015; Marabelli & Galliers, 2017). Additionally, there is limited research on the industry context. Nonetheless, Mithas, Tafti and Michell (2013) studied how the extent digital technology is used in an industry could influence a firm's choice on the use of technology. These studies provide different insights into alignment and would be interesting to investigate further.

Reference

Benbya, H., & McKelvey, B. (2006). Using coevolutionary and complexity theories to improve IS alignment: A multi-level approach. Journal of Information Technology, 21, 284–298.

Bharadwaj, A., El Sawy, O. A., Pavlou, P. A., & Venkatraman, N. (2013). Digital Business Strategy: Toward a Next Generation of Insights. MIS Quarterly, 37(2), 471–482.

Chan, Y. E., & Reich, B. H. (2007). IT alignment : what have we learned ? Journal of Information Technology, 22, 297–315.

Chanias, S., Myers, M. D., & Hess, T. (2019). Digital transformation strategy making in pre-digital organizations: The case of a financial services provider. Journal of Strategic Information Systems, 28(1), 17–33.

Ciborra, C. U. (1997). De profundis? Deconstructing the concept of strategic alignment. Scandinavian Journal of Information Systems, 9(1), 67–82.

Coltman, T., Tallon, P., Sharma, R., & Queiroz, M. (2015). Strategic IT alignment: Twenty-five years on. Journal of Information Technology, 30(2), 91–100.

Henderson, J. C., & Venkatraman, H. (1993). Strategic alignment: Leveraging information technology for transforming organizations. IBM Systems Journal, 32(1), 4–16.

Hess, T., Matt, C., Benlian, A., & Wiesböck, F. (2016). Options for Formulating a Digital Transformation Strategy. MIS Quarterly Executive, 15(2), 123–139.

Karpovsky, A., & Galliers, R. D. (2015). Aligning in practice: from current cases to a new agenda. Journal of Information Technology, 30, 136–160.

Luftman, J. (1996). Competing in the Information Age. Oxford University Press.

Luftman, J. (2000). Assessing business-IT alignment maturity. Communication of the Association of Information Systems, 4(14), 1–50.

Luftman, J., Lyytinen, K., & Zvi, T. Ben. (2017). Enhancing the measurement of information technology (IT) business alignment and its influence on company performance. Journal of Information Technology, 32, 26–46.

Marabelli, M., & Galliers, R. D. (2017). A reflection on information systems strategizing: the role of power and everyday practices. Information Systems Journal, 27, 347–366.

Mithas, S., Tafti, A., & Mitchell, W. (2013). How a firm's competitive environment and digital strategic posture influence digital business strategy. MIS Quarterly, 37(2), 511–536.

Peppard, J., & Breu, K. (2003). Beyond Alignment: A Coevolutionary View of the Information Systems Strategy

Process. International Conference on Information Systems Proceedings 61, 743–750.

Peppard, J., Galliers, R. D., & Thorogood, A. (2014). Information systems strategy as practice: Micro strategy and strategizing for IS. Journal of Strategic Information Systems, 23(1), 1–10.

Reich, B. H., & Benbasat, I. (2000). Factors that influence the social dimension of alignment between business and information technology objectives. MIS Quarterly, 24(1), 81–113.

Schlosser, F., Beimborn, D., Weitzel, T., & Wagner, H.-T. (2015). Achieving social alignment between business and IT - an empirical evaluation of the efficacy of IT governance mechanisms. Journal of Information Technology, 30, 119–135.

Sebastian, I. M., Mocker, M., Ross, J. W., Moloney, K. G., Beath, C., & Fonstad, N. O. (2017). How big old companies navigate digital transformation. MIS Quarterly Executive, 16(3), 197–213.

Smaczny, T. (2001). Is an alignment between business and information technology the appropriate paradigm to manage IT in today's organisations? Management Decision, 39(10), 797–802.

Vessey, I., & Ward, K. (2013). The dynamics of sustainable is alignment: The case for IS adaptivity. Journal of the Association for Information Systems, 14(6), 283–311.

Yeow, A., Soh, C., & Hansen, R. (2018). Aligning with new digital strategy: A dynamic capabilities approach. Journal of Strategic Information Systems, 27, 43–58.

iS
CHANNEL

ICT Occasions Changes in E-Government: The Case of Elster

Christian Poeschl

MSc in Information Systems and Digital Innovation
Department of Management
London School of Economics and Political Science

KEYWORDS

E-Government
Public Sector
Regulative Powers
Functional Simplification and Closure

ABSTRACT

The academic community has developed a vast interest in analysing information and communication technology in the public sector. Drawing on the concepts of functional simplification and closure combined with Mintzberg's forms of bureaucracy, this paper aims to investigate how technology influences processes by which decisions are made in the public administration. The analysis of the German tax declaration system, known as Elster, reveals four aspects: Elster allows faster decision making, redistributes discretionary power, makes the work of public officials more demanding and analytical, and increases the degree of formalization in the decision-making process. These findings indicate how the regulative powers of this technology are able to structure surrounding social and organisational systems. This paper concludes with a call to further analyse the role of normative agreements, such as the one epitomized by the Konsens council, in the successful deployment of technology.

Introduction

The outbreak of COVID-19 and the resulting protective measures by authorities worldwide have forced many organisations to move their operations online. The media report many different, innovative approaches on how businesses tap into the potential of information and communication technology (ICT) to continuously ensure the provision of services. Simultaneously, governments across the globe face similar challenges. The British House of Commons was headlined for proposing the introduction of a 'virtual Parliament' as a solution (BBC News, 2020). However, while such use of ICT by governments and public administrations is suddenly trending in news outlets, technology has already played an essential role throughout the last few decades. One example is the German tax declaration system, called Elster, which has contributed to the digitalisation of the finance ministry since the 1990s. Yet, news media primarily cover the changes that impact citizens. Therefore, reports about Elster's effect on the operations of the public administration have been rather scarce. Nevertheless, considering the continuing permeation of ICT in all agencies, it remains important to develop and maintain an understanding of how the public sector evolves and which implications such initiatives have. Especially, the goal of automating discretion has consequences in the delivery of public services. It creates new levels of accountability in a highly political context (Homburg, 2008). These levels often refer to the system designers behind the technology, who gain influence on how public policy is enacted on the ground.

Consequently, this paper aims to address this gap and analyse how the integration of technology into an organisational system induces changes in operational and decision-making processes. Building on the case of Elster, the author draws from multiple theories to argue that ICT does not simply increase efficiency but that certain functions are able to shape the context in which the technology is embedded. The author structures this paper as follows: After reviewing how the literature has conceptualised ICT in the public sector, the paper describes and subsequently adopts a theory-grounded approach to analyse the case study. Thereafter, the paper concludes with its findings and offers future research avenues.

Literature Review

The academic community evinced an early interest in researching e-government initiatives. Consequently, multiple schools of thought have emerged that analyse the deployment of technology in the governmental sector. A dominant proportion of the literature has conceptualised the use of ICT as a means to further rationalise public sector activities. This idea is rooted in the New Public Management (NPM) vision, which has its origins in the private sector (Gruening, 2001). While Weber's (1947) bureaucratic form initially provided organisational efficiency by enforcing hierarchical structures, division of labour and formal set of rules, an increasingly complex environment inhibits it from doing so. As the need to integrate becomes more prominent, traditional bureaucracies are incapable of achieving the same levels of efficiency given this growing uncertainty (Cordella and Tempini, 2015). Consequently, a new

Corresponding Author
Email Address: Christian.apoeschl@gmail.com

way of managing the public sector inspired by market economics has been postulated. Proponents of NPM suggest a management culture, which views citizens as customers, whose individual needs are to be satisfied. Their goal is to eliminate bureaucratic elements and use ICT to increase efficiency, effectiveness and accountability in the public sector (Dunleavy et al., 2006; Hood, 1991; Self, 2000). However, reforming the public administration to a market-based organisation affects its capabilities to provide services that follow the principles of equality and impartiality (Chapman, 1991).

As a result of this critique, academics have started to look beyond such economic outcomes. Bovens and Zouridis (2002) emphasise that the deployment of technology in the public sector transfers some discretionary power to the system architects, therefore requiring additional supervision. Cordella (2007) analyses ICT for its potential to support the bureaucratic administration in providing services in line with democratic values. He highlights that technology can both support the bureaucratic ideal of efficiency via rule-based decision making and facilitate enforcing principles of equality and impartiality (ibid.). Hence, bureaucratic organisations can be strengthened rather than radically transformed. Rather than only improving the value-for-money ratio, technology can also help to enhance the democratic process, e.g. by enabling citizens to be more directly involved in policymaking (Brewer et al., 2006). Furthermore, technology can be conceptualised as a carrier of governmental aims. Not only is the use of technology influenced by pre-existing institutional conditions (Fountain, 2001), but also its design and choice are shaped by public policies (Cordella and Iannacci, 2010). Therefore, technological artefacts both are the result of social, political and institutional negotiations and shape the enactment process.

Such influential potential of ICT is also captured by the concepts of functional simplification and closure. In contrast to the dominant literature, which focuses on instrumental terms, i.e. how technology helps to accomplish certain ends, this approach views technology as a structuring agent that supports human actions (Kallinikos, 2005). On the one hand, functional simplification involves the isolation of an operational domain, within which reality's complexity is simplified into a set of causal relationships. Although these relations can themselves be quite complex, the initial reduction of the inputs tends to make the system controllable. By further specifying how the technology handles the individual elements of this domain, it helps human actors deal with reality. The intricacies of the contemporary world are therefore broken down into piecemeal parts and their relationships to each other, i.e. the technology creates structure. On the other hand, functional closure refers to "the construction of a protective cocoon that is placed around the selected causal sequences or processes to safeguard undesired interference and ensure their recurrent unfolding" (Kallinikos, 2005, p. 190). Thus, the technological system is black-boxed and decoupled from other organisational and social spheres. Social interaction with the technology is highly limited to those with special skills, training and roles. Consequently, ICT can be seen as a regulative power that structures social and organisational interactions (Bovens and Zouridis, 2002; Kallinikos, 2005; Cordella and Tempini, 2015) as well as shapes the outcome of legislative processes (Contini and Mohr, 2014; Cordella and Gualdi, 2019).

As illustrated above, ICT in the public sector has been conceptualised in various ways. Each approach offers a slightly distinct perspective complementing the others. While the focus has been on ICT so far, its impact on different types of bureaucratic organisations must also be considered. As Mintzberg (1983) points out, bureaucracies can be differentiated based on the nature of the task, the environment and the prime coordinating mechanism. Machine bureaucracies rely on the standardisation of work processes. These organisations execute highly routine tasks in a stable environment with a high degree of formalisation. The nature of and the solution for each task can be fully determined in advance, therefore automated. On the other hand, professional bureaucracies tend to standardise skills, whereby highly trained professionals complete non-routine, complex tasks. They use human analytical skills to overcome the uncertainty and ambiguity of the complex environment. Thus, these jobs cannot be readily automated.

Drawing on the concepts of functional simplification and closure combined with Mintzberg's (1983) taxonomy, this paper aims to analyse how the deployment of technology occasions a change in the processes by which decisions are made in the public administration. Case study research may, therefore, be the most appropriate means to understand such phenomena in their natural setting (Benbasat, et al., 1987). While this research design generally allows deeper insights into the political, social and technological dimensions of e-government initiatives, this paper concentrates on the affordances of technical functionalities. The ground needed for the analysis is provided by the German tax declaration system Elster. Predominantly, secondary data sources, such as newspaper articles and online reports, were used, which were complemented by an interview with a person who has acted as Elster's public point of contact.

Case Study

Elster – an acronym for 'Elektronische Steuererklärung' – was conceptualised in 1996 and first introduced to the public in 2004. It refers to a platform that allows citizens to submit their tax data online and authorities to automatically assess and process certain tax declarations. It is managed by the tax authorities of Bavaria and is part of Konsens, a nationwide council, which aims to use ICT to integrate and standardise tax administration processes across counties (Krebs and Platzer, 2010). Additional objectives include increasing both the efficiency in processing tax declarations and the quality of the collected data.

Elster's deployment consisted of two phases. The first phase started in 2004 and required users to download the software onto their personal computers. In a

second phase at the end of 2006, Elster was available to the public as an online portal. Initially, it only offered the declaration of wage taxes, but more functionalities were added over the years to further encompass other tax forms (Krebs and Platzer, 2010). While it has been mandatory for employers to use Elster to declare taxes since 2005, private citizens still have the option to request a paper form. In 2018, over 23 million citizens opted for the paperless alternative (Elster, 2018).

Prior to digitising the tax declaration process, citizens would fill in the said paper form and send it to the tax office (Figure 1). After contractors manually transcribed the data into the computer, they would assess each declaration based on completeness. If a form was incomplete, the citizen had to be contacted for clarification. To establish whether a submission was plausible, tax officials used a guide indicating reasonable ranges for each value and their tacit knowledge and experience to come to a conclusion. Based on the decision, they would either further process the declaration or inquire additional proof (Anonymous, 2020).

Elster has changed this procedure (Figure 2). One consequence includes that the responsibility for the manual data entry has been pushed from contractors to citizens. To submit their tax declaration, citizens can now access the platform via the Internet and fill in the digitised form. The submission process can only be completed if all mandatory fields contain values, and the initial logic checks are passed. The declarations of citizens, who choose the traditional way, are still transcribed into the computer and then uploaded into Elster's database. Subsequently, the submitted declarations are first assessed by Elster's risk management software (RMS) (Link and van Dorp, 2011).

While the exact specifications of this software are confidential, its basic cornerstones are publicly available. It compares a citizen's new tax declarations with the existing database to detect any irregular developments (Hoyer, 2018). Further, the RMS uses statistical methods like the chi-squared test to analyse the number of occurrences of single digits (Olfen, 2017). The underlying idea is that every person has an unconscious preference for specific digits. Thus, if a digit appears more often or less often, the software identifies and flags these systematic deviations. The software uses these and other methods to categorise citizens into three classes (Kloth, 2010). Each class indicates a certain risk of possible tax evasion. Class 1 contains high-risk cases, which have annual earnings exceeding €500,000 or wide scope of design for declaring taxes due to the complex legal framework. For example, wealthy individuals, who have access to tax experts, may be able to circumvent certain regulations. These cases are completely analysed by a tax official. Class 2 encompasses medium risk cases.

If the RMS detects a suspicious family of values, the tax official has to assess these particular fields. Lastly, class 3 comprises low-risk cases, which are automatically processed by the system without any human intervention. Nevertheless, 2% of all declarations are evaluated manually. Furthermore, the RMS records all processing steps, thereby ensuring transparency in its operation. These measures are important to prevent fundamental errors, such as the one that occurred in 2012. It was detected that the RMS classified any work-related deductions as low-risk cases, thereby de facto waving them through the system (Kleinz, 2018). Consequently, new evaluation criteria had to be designed and incorporated into

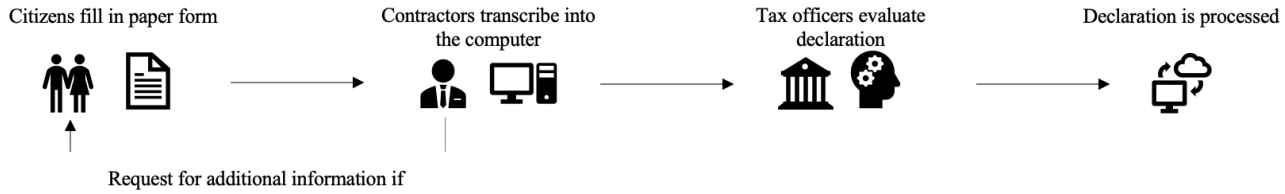


Figure 1: Traditional process

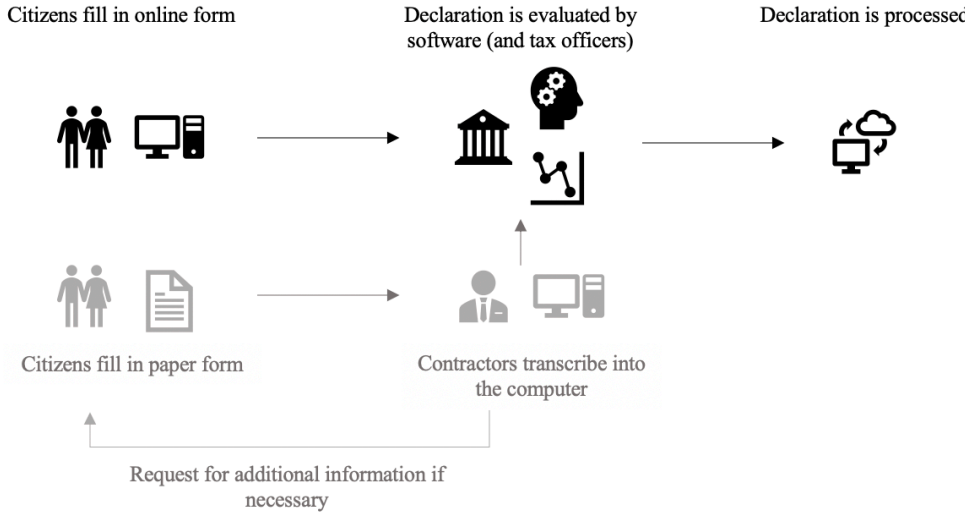


Figure 2: New process

the system. More generally, regular adaptations of the software are also required when the government changes the tax law.

Analysis

The introduction of Elster demonstrates the effort of the tax authorities to rationalise their operations. Hereby, the Konsens council provides the normative agreement that the overarching goal of all its initiatives is the standardisation in the financial administration across German states. Consequently, Elster is regarded as a contribution to this goal, as it sets the default methods for the entry, processing and storage of tax data. This not only facilitates the integration of databases across German states but also creates less room for human variance. On the side of the citizen, Elster uses coded plausibility mechanisms to ensure that the online form is filled in completely with correct values. This minimises the need for tax officials to reach out to citizens for clarification, thus saving time in the overall process and ensuring higher quality of data. To take full advantage of this improved efficiency, the government widely encourages the public to use the paperless alternative. On the side of the tax authorities, Elster's RMS assesses each declaration uniformly, therefore preventing tax officials from relying purely on their tacit knowledge.

Using Bovens and Zouridis' (2002) terminology, this technical control function further indicates a transformation from a street-level into a system-level bureaucracy. While previously, tax officials 'on the streets' had the full authority of processing tax declarations and enacted public policy through their decision-making, class 3 cases are now automatically handled by the RMS. As cases from class 1 and 2 still require human ratification, the full transformation to the system level is not yet complete. Nevertheless, this case shows how some discretionary power has shifted from the street bureaucrats to the system designer, who determines the specificities of the statistical algorithm analysing each tax declaration. As a result, a new layer in the bureaucratic process has been introduced.

As these multiple layers are associated with different tasks, they can be better analysed with Mintzberg's (1983) taxonomy. Elster and its RMS exemplify a system aimed at the automation of routine tasks. Each declaration is evaluated and then assigned to a risk category. As this evaluation is primarily based on a logical, rule-based process, Elster can be used to streamline the execution of this machine bureaucracy task. A similar task involves the final processing of cases from all classes, which does not require any advanced analytical capabilities. It includes tasks such as the upload of the data into the database or the initiation of a possible reimbursement payment. Hence, this is a simple process that is automated as well. Consequently, tax officials can concentrate their efforts on cases from class 1 and 2. Given their complexity, these cases exhibit legal intricacies that are not written in the code. Therefore, their evaluation cannot be automated by software but require more in-depth analysis and human judgment. Thus, the RMS of Elster allows tax officials to focus on professional bureaucratic tasks.

Functional Simplification and Closure

Previous notions of how technology can increase efficiency, distribute discretionary power and automate routine tasks can be complemented by the concepts of functional simplification and closure. These theoretical ideas – rather than referring to the technical artefact itself – describe the relationship with the surroundings, in which the technology operates. Hence, the focus is on the character of the very operations that define the service in its context (Kallinikos, 2009). Reviewing the whole process, a tax declaration is created by a citizen, assessed in terms of its risks by the RMS, either analysed by a tax official or directly processed.

Compared to the procedure prior to Elster's introduction, the risk assessment function has been isolated from the analogue routines. Before, public officials used their tacit knowledge to interpret the rules and guidelines. Based on their understanding, they determined the class of each tax declaration and therefore, the detail of analysis required before a decision is made. The execution of this task has now been made more formal and explicit, i.e. functionally simplified. By disaggregating human judgment into several statistical and logical operations, reality's complexity is reduced to a set of causal relationships that are standardised into sequenced scripts. For example, after analysing whether the annual earnings exceed the threshold of €500,000, the software compares the current values with previous years' values. If the percentage difference is abnormal compared to a given average delta, the software assigns the tax declaration to a higher risk class. Equally, the software allocates cases based on the results of the chi-squared test at a significance level of 0.05 or lower. All of these mathematical relationships and thresholds specify how the technology handles the individual elements of a tax declaration, thereby rendering this specific function automatable. Since the inputs and the causal connections within the operational domain are stylised, the system remains controllable to a large degree. However, as Hanseth and Ciborra (2007, p.56) point out, a consequence of this simplification is that the technology manages unexpected matters by excluding them. This also applies to the case of Elster. Its RMS relying on a finite set of statistics and pre-set conditions are not able to cope with every tax declaration. Especially cases from class 1 may take advantage of grey areas of the tax law, which are not encoded into the software. This ambiguity cannot be readily simplified into specific causal relationships, thus automated. Therefore, the system directs these particular cases to the tax official for additional assessment.

Synchronously with functional simplification, these software processes are decoupled from the broader organisational surroundings, i.e. functionally closed. The execution of the software scripts is completed without any undesired interference. The closure is achieved by highly regulating the interfaces with the system. Social contact is restricted to those individuals,

who are appointed certain roles and possess the required computational and mathematical skills (Link and van Dorp, 2011). Further, the Elster software enforces information requirements, which determine the inputs that are allowed by the system. As a consequence of this "protective cocoon" (Kallinikos, 2005, p. 190), the outcome of the software process is consistent and replicable over time. Nevertheless, a system that is functionally closed can still be changed. Elster's software is regularly adjusted to comply with current legislation. Moreover, the practice of manually cross-checking 2% of all declarations and recording each step of the process reveals erroneous outcomes, such as the one in 2012. As a result, the blackbox of the software is opened, and the corresponding simplified relationships corrected.

Thus, the concepts of functional simplification and closure illustrate how technology facilitates automation by structuring reality's complexity. As machine bureaucratic processes are already highly formalised, their structuration, and therefore automation, occurs more readily.

Therefore, the deployment of technology goes beyond what proponents of NPM postulate. Elster exemplifies that it does not simply embody a neutral means to complete existing operations more efficiently. Rather, it offers new ways of enframing and arranging pre-determined logical steps of actions, which constitute organisational procedures (Cordella and Contini, 2017). This means that the underlying character and composition of the operations of tax officials have changed through the mediation of technology, therefore influencing how organisational practices are executed.

Conclusion

The aim of this paper is to analyse how the deployment of technology occasions a change in the decision-making processes in the public sector, using the case of the German tax declaration system. As the foregoing theory-driven analysis indicates, there are noteworthy differences to the operations prior to Elster's introduction on various levels. Generally, four aspects of how a decision is reached can be highlighted.

First, Elster allows to take a decision faster. As the plausibility mechanisms ensure that citizens fill in the online form completely and appropriately, the quality of the submissions is increased, and the time spent on clarifying missing information is minimised. Therefore, more data is timely available, on which tax officials can base their decision. Moreover, Elster redistributes discretionary power. Building on Bovens and Zouridis' (2002) findings, programmers and system designers are now assigned a proportion of the authority over the tax assessment process. They design the technology that takes over some responsibilities previously assumed by tax officials. Consequently, this new division of decision-making power requires additional checks and balances, such as the random cross-checking of 2% of all declarations and the recording of each processing step. These measures allow the finance ministry to assess how computer scientists transform policies and tax legislature into code. Third, Elster makes the decision-making process of tax officials more analytical and demanding. Using Mintzberg's (1983) types of bureaucracy as a lens, tasks with different characteristics become more visible and, thus, can be separated. Routine work processes that are highly formalised can be differentiated from complex, ambiguous tasks which require analytical skills. As the simple processes are automated by Elster's system, tax officials are to deal with more intricate procedures. These require the broader knowledge and more advanced skill sets. Finally, Elster increases the degree of formalisation in the tax assessment process. As the technology simplifies a system with legal, cultural and organisational components into a set of statistical relationships and thresholds, the decision-making process becomes more explicit, and less interpretation of rules is needed. The further closure of the technical system fends off interference from the surrounding environment and ensures consistent execution of the operation. As a result, a more homogeneous assessment is achieved, which simultaneously enforces the principles of equality and impartiality in the delivery of public services to a larger extent.

Therefore, Elster can be seen as a good e-government initiative which is designed as a support for professional bureaucracies and which strengthens democratic values. Hereby, the Konsens council plays a major role as it provides the overarching normative agreement. It thus aligns the legislature and the different agencies with paving the way for Elster's deployment.

However, these research findings have to be seen in light of some limitations. First, the data collection method provides only limited insights into the workings of the public administration. As mostly secondary data sources were used, such as news articles and online reports, their narratives may be biased towards their targeted readership. To overcome this limitation, an interview with a contact person for Elster was conducted to reveal a more detailed account of the operations of tax officials. Additional interviews could not be conducted due to the emergent COVID-19 situation. Consequently, aspects like the involvement of tax officials in the design of the software, the prevalent social system in the office or the influence of Konsens could not be clarified. Therefore, future studies could provide deeper insights into the role of such normative agreements in the implementation of technology in public organisations. As the research question focuses on procedural changes, the notions of functional simplification and closure combined with the idea of different bureaucratic forms provided a suitable lens through which to analyse the impacts of Elster on an operational level. However, other aspects, such as the perceptions, opinions and interests of individual public officials, are not addressed. A further avenue of research could shed light on how agents actually enact Elster's technology, therefore influencing policy-making on the streets.

Reference

Anonymous, 2020. Elster Contact Person [Interview] (17 February 2020).

BBC News, 2020. Coronavirus: Commons Speaker calls for 'virtual Parliament'. [Online] Available at: https://www.bbc.com/news/uk-politics-52128495 [Accessed 05 April 2020].

Benbasat, I., Goldstein, D. & Mead, M., 1987. The Case Research Strategy in Studies of Information Systems. MIS Quarterly, 11(3), p. 369–386.

Bonina, C. & Cordella, A., 2008. The new public management, e-government and the notion of 'public value': lessons from Mexico. Paris, Association for Information Systems.

Bovens, M. & Zouridis, S., 2002. From street-level to system-level bureaucracies: How information and communication technology is transforming administrative discretion and Constitutional Control. Public Administration Review, 62(2), p. 174–184.

Brewer, G. A., Neubauer, B. J. & Geiselhart, K., 2006. Designing and Implementing E-Government Systems: Critical Implications for Public Administration and Democracy. Administration & Society, 38(4), p. 472–499.

Bundesministerium der Finanzen, 2016. Gesetze und Gesetzesvorhaben. [Online] Available at: https://www.bundesfinanzministerium.de/Content/DE/Gesetzestexte/Gesetze_Gesetzesvorhaben/Abteilungen/Abteilung_IV/18_Legislaturperiode/Gesetze_Verordnungen/2016-07-22-Steuermodernisierungsgesetz/0-Gesetz.html [Accessed 03 April 2020].

Chapman, R., 1991. Concepts and Issues in Public Sector Reform: the Experience of the United Kingdom in the 1980s. Public Policy and Administration, 6(2), p. 1–19.

Contini, F. & Mohr, R., 2014. How the Law Can Make It Simple: Easing the Circulation of Agency in e-Justice. In: Contini, F. & G. Lanzara, eds. The Circulation of Agency in E-Justice. Dordrecht: Springer, pp. 53-78.

Cordella, A. & Bonina, C., 2012. A public value perspective for ICT enabled public sector reforms: A theoretical reflection. Government Information Quarterly, 29(4), p. 512–520.

Cordella, A. & Contini, F., 2017. Law and Technology in Civil Judicial Procedures. In: R. Brownsword, E. Scotford & K. Yeung, eds. The Oxford Handbook of Law, Regulation and Technology. Oxford: Oxford University Press, pp. 247-250.

Cordella, A. & Gualdi, F., 2019. Law, Technology and Policies: A Complex Negotiation To Generate Value. New York, ICEEG.

Cordella, A. & Iannacci, F., 2010. Information systems in the public sector: The e-Government enactment framework. Journal of Strategic Information Systems, 19(1), p. 52–66.

Cordella, A. & Tempini, N., 2015. E-government and organizational change: Reappraising the role of ICT and bureaucracy in public service delivery. Government Information Quarterly, 32(3), p. 279–286.

Cordella, A., 2007. E-government: towards the e-bureaucratic form?. Journal in Information Technology, Volume 22, pp. 265-274.

Dunleavy, P., Margetts, H., Bastow, S. & Tinkler, J., 2006. New public management is dead - long live digital-era governance. Journal of Public Administration Research and Theory, 16(3), pp. 467-494.

Elster, 2018. Elster - Ihr Online Finanzamt. [Online] Available at: https://www.elster.de/eportal/infoseite/presse [Accessed 11 April 2020].

Fountain, J., 2001. Building the Virtual State: Information Technology and Institutional Change.. Washington, DC: Brookings Institution Press.

Gruening, G., 2001. Origin and theoretical basis of New Public Management. International Public Management Journal, Volume 4, p. 1–25.

Hanseth, O. & Ciborra, C., 2007. Risk, Complexity and ICT. Cheltenham, UK: Edward Elgar Publishing.

Hildebrandt, M., 2008. Legal and Technological Normativity: more (and less) than twin sisters.. Techné: Research in Philosophy and Technology, 12(3), p. 169–183.

Homburg, V., 2008. Understanding E-Government: Information System in Public Administration. New York: Routledge.

Hood, C., 1991. A public management for all seasons?. Public Administration, 69(1), p. 3–19.

Hoyer, N., 2018. Wirtschaftswoche. [Online] Available at: https://www.wiwo.de/finanzen/steuern-recht/grosser-praxistest-die-beste-steuersoftware-fuer-ihr-geld/21099576.html [Accessed 15 March 2020].

Kallinikos, J., 2005. The order of technology: Complexity and control in a connected world. Information and Organisation, Volume 15, pp. 185-202.

Kallinikos, J., 2009. The regulative regime of technology. In: ICT and innovation in the public sector. London: Palgrave Macmillan, pp. 66-87.

Kleinz, T., 2018. Algorithmen Ethik. [Online] Available at: https://algorithmenethik.de/2018/03/27/das-automatische-finanzamt/ [Accessed 15 March 2020].

Kloth, R., 2010. bdp aktuell. [Online] Available at: https://www.bdp-team.de/steuerberatung/risikomanagement-der-finanzverwaltung-big-brother-beobachtet-dich [Accessed 15 March 2020].

Krebs, R. & Platzer, B., 2010. ELSTER - Meilensteine eines erfolgreichen eGovernment-Projektes, Munich: Bayerisches Landesamt für Steuern.

Link, P. & van Dorp, T., 2011. Steuerliches Risikomanagement. Arbeit und Arbeitsrecht, 11(13).

Mintzberg, H., 1983. Structure in fives: designing effective organizations. London: Prentice Hall.

Moore, M., 1995. Creating public value : strategic management in government. Cambridge, Mass: Harvard University Press.

Olfen, M., 2017. Olfen Meinecke Vögler. [Online] Available at: https://www.steuern-und-strafe.de/chi-quadrat-test-hilfsmittel-der-betriebsprufung/ [Accessed 15 March 2020].

Pang, M., Lee, G. & Delone, W., 2014. IT resources, organizational capabilities, and value creation in the public-sector organizations: public-value management perspective. Journal of Information Technology, 29(3), p. 187–205.

Self, P., 2000. Rolling Back the State: Economic Dogma & Political Choice. New York: St. Martin's Press.

Weber, M., 1947. The theory of social and economic organization. New York: Oxford University Press.

Information Systems and Innovation within the Department of Management

Within LSE's Department of Management, we form the leading European university-based research cluster focusing on Information Systems and Innovation, and are recognised widely as amongst the top ten such clusters in the world. We have 12 full-time academics and benefit from the contributions of Visiting Professors, all of whom are scholars of international repute and leaders in the field, from Visiting Fellows who are experts in their respective fields, and from project researchers and our PhD students. Faculty are active in the International Federation of Information Processing (IFIP), the Association for Information Systems (AIS), the UK Academy for Information Systems (UKAIS), the British Computer Society (BCS), and other national and international organizations including United Nations and European Union bodies. They are Editors-in-Chief of major journals including JIT, ITP) and variously serve as Senior and Associate Editors on most high quality refereed journals in the IS field (e.g. MISQ, MISQE, ISR, EJIS, ISJ plus over 20 others).

Teaching in Information Systems has been rated as excellent by the UK's Quality Assurance Agency and its research is recognized as internationally excellent by the Higher Education Funding Council for England. Awards and recognition are extensive and include Frank Land's Leo award of the AIS for Lifetime Exceptional Achievement, Ciborra's AIS Distinguished Member award, and Willcocks's Price Waterhouse Coopers/Corbett Associates World Outsourcing Achievement award for academic contribution to this field.

The Department of Management runs several high profile Information Systems seminar programmes. These include the annual Social Study of ICTs seminar run over two days in March which attracts over 200 international participants and has a related two day research workshop.

Information Systems faculty are actively involved in the delivery of two degree programmes offered within the Department of Management – a one-year MSc in Management, Information Systems and Digital Innovation of (MISDI) and a PhD in Information Systems. In addition they provide Information Systems knowledge within the core management BSc and MSc courses within the department. These Faculty's research, teaching and dissemination strategies are closely interlinked and their distinctive focus on the social study of Information Communication Technologies (ICTs) and Innovation underlies a concern for policy and practice issues in six major fields (see figure). The MSc in Management, Information Systems and Digital Innovation (MISDI) draws on all items.

LSE Information Systems Alumni Group (LISA)

LISA is the Information Systems and Innovation Group's official alumni group. It is dedicated to establishing, maintaining and forging new relationships between alumni, industry and the Group. It is open to any alumni of the Group's programmes (ADMIS, ISOR, MISI, MISDI, PhD) and is supported by staff within the Group. LISA has over 1000 members globally and is expanding through its regular activities. LISA regularly organises events for alumni and current students and provides opportunities to network, socialise and learn. This year's LISA conference highlighted relevant developments in FinTech. The four speakers, Julia Doukaki, Oleh Stupak, Joyce Li and Gabriel Karageorgiou, all of which are experts in their individual fields, were highly requested and tested by the audience. Experiences and ideas were shared and captured by the two MISIDI students Christian Poeschl and Maximilian Goehmann acting as moderators. By scanning the QR code, you can watch the recording of the live stream on Facebook.

To know more about latest events organised by LISA and connect with LISA members all across the globe join us on Facebook and LinkedIn:

- LISA on Facebook – https://www.facebook.com/groups/LSE.IS.Alumni/

- LISA on LinkedIn – https://www.linkedin.com/company/lse-information-systems-alumni-lisa-/

If you wish to contribute or participate in our activities, kindly get in touch with the LISA representative Heemanshu Jain (MSc 2008-09) via heemanshu@alumni.lse.ac.uk

LSE Department of Management

LISA LSE Information Systems Alumni