Towards a Framework for the Adaptation of the Internet of Things in International Border Control Organizations

Paul Brous, Monica den Boer, Pascal Wolf

Towards a Framework for the Adaptation of the Internet of Things in International Border Control Organizations

Paul Brous[1][0000-0002-0593-1168] , Monica den Boer[2] and Pascal Wolf[2]

[1] Legend Data Management, 3053WX Rotterdam, Netherlands
[2] Nederlandse Defensie Academie, Kraanstraat 4, 4811XC Breda, Netherlands
paul.a.brous01@gmail.com
mgw.d.boer@mindef.nl
pr.wolf.01@mindef.nl

Abstract. COVID-19, BREXIT, global terrorism, and political ideologies such as "America First" have increasingly laid bare ethical, political and operational stresses attached to international border crossings. Organizations tasked with the management of international borders are having to cope with new threats to border management and more and more are choosing to incorporate the Internet of Things (IoT) technologies within their border management processes as a means of governing mobility. However, whilst the introduction of IoT can introduce a number of benefits, the adaptation of new technologies presents substantial challenges to border management organizations and can introduce a number of unforeseen risks such as encroachment on the rights of the individual, lack of transparent governance, absence of legal legitimacy, opaque delegation of responsibilities between communitarian organizations and unethical decision-making or behavior. This article proposes a framework for the adaptation of IoT by border management organizations which aims at helping border management organizations overcome the challenges presented by the implementation of IoT. The implementation of this framework includes wide-ranging changes to the structure of the organization, changes to processes and systems, and changes to the continuous training and development of staff members.

Keywords: IoT, Internet of Things, Border Management, Risks, Benefits

1 Introduction

COVID-19, global terrorism, BREXIT and political movements such as "America First" have increasingly laid bare ethical, political and operational stresses facing the government of international border crossings. In the face of heightened political pressure, organizations tasked with the management of international borders are having to cope with new threats to border management, despite traditional constraints such as limited budgets and reduced staff. As such, countries are increasingly choosing to digitalize the government of international borders by incorporating Internet of Things (IoT) technologies within their border management processes [1] as a means of

improving the governance of mobilities [2] and improving the policing and security of international borders [3].

The IoT is a network of objects that communicate between themselves and other internet-enabled devices over the Internet allowing organizations to monitor and control the physical world remotely [4], [5]. However, border management organizations face unique challenges to IoT implementation, such as the large numbers of people and goods which cross international borders, the large areas which need to monitored and secured [6], and the need for international cooperation [7]. Furthermore, border management organizations are choosing more often for a pre-liminal and post-liminal approach to border security as opposed to a liminal approach. Whilst the introduction of IoT can introduce a number of benefits for border management purposes, the delegation of control to technology and the increasing lack of physical presence presents substantial challenges and can introduce a number of unforeseen risks such as encroachment on the rights of the individual, lack of transparent governance, lack of legal legitimacy, opaque delegation of responsibilities between organizations, unethical decision-making or behavior [8] and a mutual lack of trust.

Despite the popularity of IoT technology for border management, particularly with regards to biometrics such as fingerprint scanners, facial recognition or iris scanners, the adoption of such technologies has proved in the past to be challenging for border management organizations [9], [10]. The reasons for these failures are often due not to technological deficiencies but are often more rooted in social aspects. For example, because maritime rescue services are not part of EUROSUR, border guards do not necessarily share information with them due to ill-defined responsibilities within Europe [9]. Furthermore, despite the growing number of investigations into the technological possibilities of smart borders, little research has been done on the social impact of IoT implementation, in particular as to its impact on border management organizations as well as their inter-organizational relationships. This article addresses this knowledge gap by discussing a review of background literature and proposing a framework for the adaptation of IoT by border management organizations.

This research investigates the impact of IoT implementation on border management organizations using Duality of Technology theory [11] as underlying logic. The central question asks what conditions border management organizations should take into account when adapting IoT for the digitalization of border government? This article proposes a framework for the adaptation of IoT by border management organizations and concludes that implementing this framework requires organizations to develop capabilities which ensure that the introduction of IoT fits the purposes of border control whilst also mitigating the accompanying risks to the border management organization. The development of these capabilities may include wide-ranging changes to the structure of the organization, changes to processes and systems, and changes to the continuous training and development of staff members.

This article reads as follows, in section two of this article the methodology followed to develop the framework for adaptation of IoT for border management on the basis of propositions developed in a systematic review of literature is described. In section three the systematic review of literature is described and propositions for a framework of IoT adaptation for border management are synthesized. In section four a framework for the

adaptation of the IoT for border management organizations is described and discussed. In section five, conclusions are drawn and proposals are made for further research.

2 Methodology

The proposed framework for IoT adaptation for border management organizations was developed on the basis of a systematic review of background literature. This literature review follows the method proposed by Webster & Watson [12] and synthesizes literature with regards to the adaptation of IoT by border management organizations. Our research objective is to understand under what conditions IoT can best be adapted by border management organizations. However, there is only limited research on IoT adaptation for border management and models for the adaptation of IoT in border management organizations are missing This article fills this gap by describing a framework for IoT adaptation by border management organizations. The framework can be used by border management organizations to coordinate the successful adaptation of IoT and mitigate the negative impact of IoT implementations. Duality of technology theory [11] was used as underlying logic to order and analyze relevant literature in order to ensure sufficient coverage of essential topics. Based on Giddens' [13] theory of structuration, duality of technology [11] describes technology as assuming structural properties whilst being the product of human action. Orlikowski identifies four main relationships, namely: 1) technology as a product of human agency, 2) technology as a medium of human agency, 3) organizational conditions of interaction with technology and, 4) organizational consequences of interaction with technology. Using duality of technology theory as basis for the literature review serves to help us understand what adaptation of IoT for border management entails by providing a multi-perspective analysis of the phenomenon.

As suggested by Webster & Watson [12], the review of literature is limited to the adaptation of IoT by border management organizations, although due to the importance of interactions between cross-border organizations, these relationships have also been taken into consideration. Furthermore, because the adaptation of IoT for border management is a relatively new phenomenon, the literature review is restricted to literature published after 1999. The literature review was also limited to the databases Scopus, Web of Science and Google Scholar. On the 27th of February 2021, the search string ("Internet of Things" AND ("border management" OR "border control" OR "mobility governance" OR "border policing") AND "organizations") returned 684 hits. Forward and backward searches were conducted until saturation of information was achieved. Based on this consideration, a selection of 31 relevant articles was made based on the criteria that they specifically address the influence or impact of IoT applications on border management organizations and digital border government. When articles dealt with similar technologies or had similar conclusions, the most recently published article was selected for inclusion. The articles were then organized according to the logic provided by duality of technology theory in order to generate the requirements for the framework of IoT adaptation for border management

organizations, and propositions which form the basis of the framework were synthesized out of the grouped literature.

3 Literature Review

According to Scholl [14, p. 1], digital government includes, "the use of information technology to support government operations, engage citizens, and provide government services". Border management organizations across the world are increasingly adapting digital technologies to support the interaction between travelers and border officials. According to Lindgren et al. [15] the adaptation of emerging technologies such as IoT helps fulfill the primary goals of digital government such as improving efficiency and service quality as well as increasing government transparency concerning, for instance, the search criteria that are being applied. The situation whereby a form of ubiquitous artificial intelligence is created by networking physical objects over the internet is commonly referred to as the IoT [16]. The automated generation and analysis of data provided by the IoT is often of better quality than traditional data generated by traditional means, is often more timely and has substantially larger volumes [17]. As such, much of the value of IoT is derived from the data the IoT produces [1]. As the concept of smart borders is data intensive [8], IoT has a large potential to improve the digital government of international borders [18] through the policing of international borders [19] such as using artificial intelligence to detect patterns in smuggling routes, improving mobility management [20] through the use of wifi-based pax tracking or check-in touchpoints for example the management of migration [21] through the use of entry decision-making engines, and improving support processes through data driven border management.

However, the development and use of IoT data and applications carries risk and is reliant on a number of conditions which are often more social in nature such as the need to ensure privacy [22] and security [19] and the need to maintain public trust and transparency [21], but also are related to organizational change such as the need for new skills and business processes [23]. This means that a mix of variant conditions are to be met prior to the border management adaptation process.

3.1 IoT as a medium of human agency in border management applications

IoT as a medium of human agency [11] takes the perspective that IoT is used by border management organizations in particular use cases to improve the efficiency or effectiveness of their processes or, for example, to reduce overhead, arbitrary decision-making, and lower costs. Due to the particular challenges facing border management organizations such as the need to monitor and control vast and sometimes sparsely populated border areas in a wide variety of conditions, as well as the need to protect the security of the many whilst ensuring the privacy and dignity of the individual, border management organizations are more frequently turning to automated IoT solutions to find solutions to these challenges. Table 1 below presents the popular uses for IoT in

border management organizations. As such the framework for IoT adaptation for border management organizations should include these use domains.

Table 1. Uses of IoT for Border Management Organizations

Business Domain	IoT Use Domain	Literature
Border policing	• Predictive and prescriptive border policing (e.g. with regards to trafficking)	[10], [24], [25]
	• Non-invasive inspection	[6], [21]
	• Monitoring and surveillance	[9], [10], [19], [25]
	• Corruption prevention	[19], [26]
	• Fraud detection	[21], [26]
Mobility Governance	• Migrant tracking and control	[2], [9], [10], [21], [27]
	• Health inspection	[21], [27]
	• Identification and authentication management	[2], [21], [28]–[30]
	• Seamless flow	[21], [27]
	• Asylum management	[6], [31]
	• Irregular immigration	[6], [7], [9], [25]
	• Identifying criminals and fugitives	[20], [27], [32]
Border Security	• Crowd detection and management	[1]
	• Individual/personal security	[21]
	• Calamity prevention and control	[1]
	• Asset security	[6]
	• Cyber security	[19]
	• Weapons guidance	[1]
	• Anti-terrorism intelligence	[2]
	• Situational awareness	[1]
Support	• Logistics	[1]
	• Predictive maintenance	[1]
	• Fleet monitoring and management	[1]
	• Individual supplies	[1]
	• Workforce training and healthcare	[1]

More and more, border management organizations tend to focus their management processes on the generation of intelligence which allows them to predict and prescribe actions with regards to border policing [10], mobility governance [27], and border security [1], as well as improving necessary support processes such as logistics. This suggests that the digitalization of the border government process through IoT adaptation may improve the efficiency of operational and tactical processes. As such, proposition 1 reads as follows: *border management organizations which adapt IoT for border management purposes are more likely to have improved operational and tactical border management processes*.

3.2 IoT as a product of human agency in border management applications

IoT implementation projects in the past have not always been successful [9] as border management organizations have technological requirements which are specific to the border management domain. In addition to physical, economic and geographic requirements border management organizations also have to take complex issues into consideration such as national security and political pressures. This often requires border management organizations to develop and manage bespoke solutions in-house. Adaptation of IoT technology for border management is therefore often a complex undertaking. Table 2 below presents necessary adaptation issues of IoT for border management organizations. As such the framework for IoT adaptation for border management organizations should include these product development domains.

Table 2. Development of IoT for border management

Business Domain	IoT Product Domain	Literature
IT Management	• Redesign of Information Technology (IT) infrastructure	[1], [32]–[35]
	• Scalability	[32], [33]
	• Energy efficiency	[1]
	• Sensor development	[1], [33], [34]
	• Interoperability	[1], [10], [28], [33]
	• Rapid deployment	[1], [33]
	• Accessibility	[34]
	• Connectivity	[1], [32], [33]
Data Management	• Redesign of data infrastructure	[29], [30]
	• Digital security	[32], [33]
	• International cyber security	[7], [36], [37]
	• Sensor calibration	[1], [33], [34]
	• Bias detection	[29], [30]

Many of the challenges associated with IoT adaptation are considered to be of a technical nature, particularly with regards to digital security[32], but it is often in the (mis)use or analysis of the data in which the failures of IoT implementations in border management settings occur [30]. This suggests that achieving the efficiency goals of digital border government may require that border management organizations address data and IT management considerations. As such, proposition 2 reads as follows: *border management organizations with mature IT and data management processes are more likely be able to successfully adapt IoT for border management purposes*.

3.3 Organizational conditions of interaction with IoT in a border management context

Due to the complexity of IoT adaptation for border management successful IoT implementations require a number of organizational conditions to be met before implementation can occur in an operational setting. Modern border management is no

longer a question of simply monitoring travelers at a single point of entry. The traveler's journey often begins before they have left home as many border crossings worldwide require such things as passports and visas. Contemporary border management is a combination of off-shore migration management, border crossing management and in-country mobility management and this requires not only interdepartmental coordination, but also international and inter-organizational cooperation. Table 3 below presents necessary organizational conditions for adaptation of IoT for border management organizations. As such the framework for IoT adaptation for border management organizations should include the fulfilment of these organizational conditions.

Table 3. Organizational conditions for IoT adaptation in border management organizations

Business Domain	Organizational condition	Literature
IT Governance	• Security framework (including budget, staff, processes, standards, policies, technology)	[19], [22], [34]
	• Technical framework (including budget, staff, processes, international standards, policies)	[26], [33]–[36]
	• Systemization of administrative policies	[10], [20], [33]
Data Governance	• Legal frameworks for data collection, storage and analysis	[20], [21], [32], [34], [37]
	• Data quality management	[16], [19], [37]
	• Data protection (privacy) framework (including budget, staff, processes, standards, policies, technology)	[19], [22], [26], [28], [34]
	• Data access management	[19], [32], [38]
	• Data sharing framework (including budget, staff, processes, standards, policies, technology)	[19], [26], [32], [38], [39]
	• International cooperation frameworks	[32], [33], [36], [39]
	• Interorganizational cooperation frameworks	[10], [33], [38]
	• Interdepartmental cooperation	[10], [26], [33]
	• Data ethics framework	[10], [21], [34], [37]

Although the technical challenges of IoT adaptation are myriad, the importance of the data governance domain is often overlooked in implementation projects [22]. Data governance has been shown to be a vital component of successful artificial intelligence initiatives [40]. This suggests that IT governance and data governance may be essential processes for achieving the objectives of digital border government. As such proposition 3 reads as follows: *border management organizations with mature IT and data governance processes are more likely able to successfully adapt IoT for border management purposes*.

3.4 Organizational consequences of interaction with IoT in a border management context

Once IoT has been adapted and implemented in a border management setting, many border management organizations are in turn faced with consequences which are often unanticipated and which, in turn, need to be managed. For example, the simple act of creating a new border entry point can create large changes in migration patterns. Table 4 below presents necessary potentially unforeseen organizational consequences of adaptation of IoT for border management organizations. As such the framework for IoT adaptation for border management organizations should include the taking into account of these consequences.

Table 4. Organizational consequences of IoT adaptation for border management organizations

Business Domain	Organizational consequence	Literature
Direct organizational consequences	• New skills required, some skills become obsolete	[40], [41]
	• New departments required, some departments become obsolete	[40], [41]
	• New business processes required, some processes become obsolete	[40], [41]
	• Higher support costs	[21], [26], [34], [35], [42]
Indirect organizational consequences	• Lack of public trust	[8], [19], [26], [36]
	• Reduced transparency	[8], [19], [36]
	• Incorrect digital profiling/ chances of bias	[21], [29], [31]
	• Changing mobility patterns	[10], [32]
	• Heightened biopolitics	[21], [31]
	• Heightened chance of discrimination	[21], [31]

Implementation projects often necessarily focus on short-term goals and gains due to time and budgetary constraints [21]. However, many of the changes wrought by the implementation of IoT in border management settings can have long-term consequences for the public and for the border management organization itself. This suggests that border management organizations may need to be aware of these potential long-term consequences before IoT implementation occurs in order to be able to mitigate these consequences and achieve their digital border government goals. Proposition 4 therefore reads as follows: *border management organizations which are aware of the direct and indirect consequences of IoT are more likely to be able to adapt IoT for border management purposes in a sustainable fashion.*

4 A Proposed Framework for IoT Adaptation for Border Management Organizations

The review of background literature synthesized four propositions for the adaptation of IoT for border management organizations. Proposition 1 proposes that IoT may be

adapted for use in border management operations. The literature review provides a plethora of potential use cases such as the use of IoT for border policing, border security, mobility governance and support. In order for these use cases to be implemented, IoT technology needs to be adapted for use in a border management setting. Proposition 2 proposes that IoT needs to be specifically developed for border management as border management organizations have specific requirements such as the need for international cooperation. The use of IoT in border management is also only possible if certain organizational conditions are met. As such, proposition 3 proposes that IoT initiatives in border management settings are more likely to be successful if these organizational conditions are met. As a result of meeting these requirements and implementing IoT applications, proposition 4 proposes that many border management organizations are faced with consequences which are often unanticipated and which, in turn, need to be managed. These propositions follow the underlying logic of duality of technology theory [11] and are included in the framework as depicted by figure 1 below.

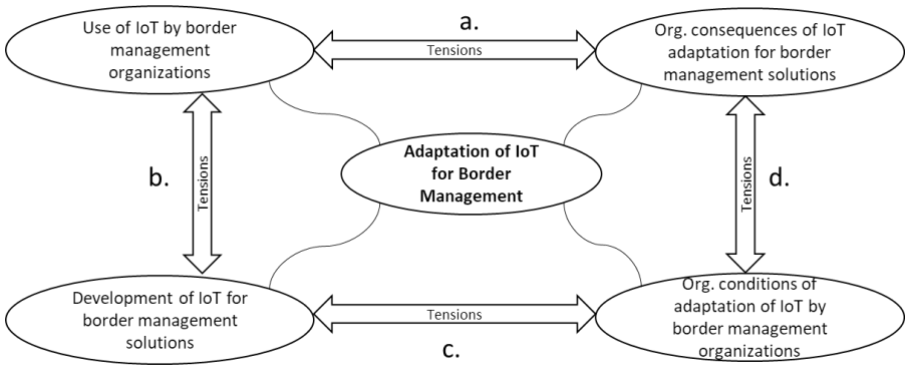

Fig. 1. A proposed framework for IoT adaptation for border management organizations

The framework of IoT adaptation for border management organizations as depicted in figure 1 above shows that tensions arise between each of the four focus domains. These tensions have been lettered 'a' through to 'd' and are explained as follows:

a) Effective use of IoT in border management situations requires legal and ethical frameworks, skilled staff, well-managed technology and new business processes, however, consequences such as privacy and security considerations can also constrain the use of IoT in border management.
b) IoT can only be used once it has been implemented, but IoT is generally only implemented once specific application to cases has been identified.
c) Adaptation of IoT for border management solutions requires innovative knowledge, new departments, additional staffing and greater investments in IT in border management organizations on the short term, however, on the long term the results may contribute to efficiency gains and cost reductions in operations.

d) Adaptation of IoT requires new legal frameworks, skills, processes and technology, but once implemented may cause other skills, staff and processes to become obsolete.

Many IoT applications in border management settings have not achieved the effect initially desired by the organization or have introduced unforeseen complexities for the organization. Moreover, costs of IoT implementations are often deemed exorbitant. The proposed framework as depicted above in figure 1 allows border management organizations to become aware of the conditions as well as tensions in the development of IoT as well as its implementation in an operational setting. A smart anticipation to these tensions allows border management organizations to decide on ways to mitigate accompanying risks and ensure that necessary organizational conditions have been met before being confronted by these risks in a post-pilot setting.

5 Conclusion

Border management organizations need to adapt IoT before use in border management situations. This adaptation of IoT introduces changes into the border management organization. In this article we applied the duality of technology theory [11] to the adaptation of IoT for border management and confirmed the dual nature of IoT in border management settings. The majority of studies on IoT in border management tend to focus on a single dimension such as the use of IoT for border management purposes, however, confirmation of the duality of IoT in border management shows that adaptation of IoT for border management is multi-dimensional. This means that when border management organizations choose to adapt IoT for their purposes, they need to understand how IoT adaptation will in turn structure the organization or introduce potentially unexpected risks before, during and after a border management pilot programme.

Based on a review of background literature, this article synthesized four propositions which were used to form the basis of the proposed framework. While this article is limited to a literature review, further research is recommended in order to test the propositions and the framework in a real-life setting. This direction can hardly be regarded as a luxury, given the high speed of developments in the arena of border management, where border control starts at home and only stops when one has reached his or her destination.

6 References

1. P. Fraga-Lamas, T. Fernández-Caramés, M. Suárez-Albela, L. Castedo, and M. González-López, “A Review on Internet of Things for Defense and Public Safety,” *Sensors*, vol. 16, no. 10, p. 1644, Oct. 2016, doi: 10.3390/s16101644.
2. L. Amoore, “Biometric borders: Governing mobilities in the war on terror,” *Political geography*, vol. 25, no. 3, pp. 336–351, 2006.

3. P. Lehtonen and P. Aalto, “Smart and secure borders through automated border control systems in the EU? The views of political stakeholders in the Member States,” *European Security*, vol. 26, no. 2, pp. 207–225, 2017.
4. van Kranenburg R. et al. (2014) Co-creation as the Key to a Public, Thriving, Inclusive and Meaningful EU IoT. In: Hervás R., Lee S., Nugent C., Bravo J. (eds) Ubiquitous Computing and Ambient Intelligence. Personalisation and User Adapted Services. UCAmI 2014. Lecture Notes in Computer Science, vol 8867. Springer, Cham. https://doi.org/10.1007/978-3-319-13102-3_65.
5. C. Ramos, J. C. Augusto, and D. Shapiro, “Ambient Intelligence-the Next Step for Artificial Intelligence,” *IEEE Intelligent Systems*, vol. 23, no. 2, pp. 15–18, Mar. 2008, doi: 10.1109/MIS.2008.19.
6. M. H. U. Sharif *et al.*, “Physical Security Practices On International Border Management,” *Sci.Int.*, vol. 31, no. 3, pp. 525–528, 2019.
7. R. Koslowski, “International Cooperation to Create Smart Borders,” in *Conference on North American Integration: Migration, Trade and Security, Ottawa, Canada*, 2004, vol. 1, no. 2.
8. M. Den Boer, “Trusted Travellers: Managing Mobility in Challenging Times,” in *Trust in International Police and Justice Cooperation*, 1st ed., S. Hufnagel and C. McCartney, Eds. Oxford: Hart Publishing, 2017, pp. 77–96.
9. B. Hayes and M. Vermeulen, “The EU’s New Border Surveillance Initiatives,” Brussels, Belgium, 2012.
10. Ö. E. Topak, C. Bracken-Roche, A. Saulnier, and D. Lyon, “From smart borders to perimeter security: The expansion of digital surveillance at the Canadian borders,” *Geopolitics*, vol. 20, no. 4, pp. 880–899, 2015.
11. W. J. Orlikowski, “The Duality of Technology: Rethinking the Concept of Technology in Organizations,” *Organization Science*, vol. 3, no. 3, pp. 398–427, Aug. 1992, doi: 10.1287/orsc.3.3.398.
12. J. Webster and R. T. Watson, “Analyzing the Past to Prepare for the Future: Writing a Literature Review,” *MIS quarterly*, vol. 26, no. 2, pp. 13–23, Jun. 2002.
13. A. Giddens, “New rules of sociological method: A positive critique of interpretative sociology,” *London: Hutchinson*, 1976.
14. H. J. Scholl, “Digital Government: Looking Back and Ahead on a Fascinating Domain of Research and Practice,” *Digit. Gov.: Res. Pract.*, vol. 1, no. 1, p. 7:1-7:12, Feb. 2020, doi: 10.1145/3352682.
15. I. Lindgren, C. Ø. Madsen, S. Hofmann, and U. Melin, “Close encounters of the digital kind: A research agenda for the digitalization of public services,” *Government Information Quarterly*, vol. 36, no. 3, pp. 427–436, Jul. 2019, doi: 10.1016/j.giq.2019.03.002.
16. P. Brous and M. Janssen, “Advancing e-Government Using the Internet of Things: A Systematic Review of Benefits,” in *Electronic Government*, E. Tambouris, M. Janssen, H. J. Scholl, M. A. Wimmer, K. Tarabanis, M. Gascó, B. Klievink, I. Lindgren, and P. Parycek, Eds. Thessaloniki: Springer International Publishing, 2015, pp. 156–169.
17. P. Brous, M. Janssen, and P. Herder, “The dual effects of the Internet of Things (IoT): A systematic review of the benefits and risks of IoT adoption by organizations,”

International Journal of Information Management, vol. 51, p. 101952, Apr. 2020, doi: 10.1016/j.ijinfomgt.2019.05.008.

18. M. Liutkevičius, K. I. Pappel, S. A. Butt, and I. Pappel, "Automatization of Cross-Border Customs Declaration: Potential and Challenges," in *Electronic Government*, Cham, 2020, pp. 96–109, doi: 10.1007/978-3-030-57599-1_8.
19. P. Cooke, "'Digital tech' and the public sector: what new role after public funding?," *European Planning Studies*, vol. 25, no. 5, pp. 739–754, May 2017, doi: 10.1080/09654313.2017.1282067.
20. I. Vrăbiescu, "Deportation, smart borders and mobile citizens: using digital methods and traditional police activities to deport EU citizens," *Journal of Ethnic and Migration Studies*, pp. 1–18, 2020.
21. M. Abomhara, S. Y. Yayilgan, L. O. Nweke, and Z. Székely, "A comparison of primary stakeholders' views on the deployment of biometric technologies in border management: Case study of Smart Mobility at the European land borders," *Technology in Society*, vol. 64, p. 101484, 2021.
22. P. Martí, X. Morales, S. Mantzagriotis, and L. Tadesse, "Awareness of the Internet of Things research regarding security and privacy risks," *Meta-Research*, p. 74, 2018.
23. P. Brous, M. Janssen, and P. Herder, "Internet of Things adoption for reconfiguring decision-making processes in asset management," *Business Process Management Journal*, 2018.
24. S.-B. Kim and D. Kim, "ICT Implementation and Its Effect on Public Organizations: The Case of Digital Customs and Risk Management in Korea," *Sustainability*, vol. 12, no. 8, p. 3421, 2020.
25. M. Bhattacharya and A. Roy, "Smart Border Security System Using Internet of Things," in *International Conference on Computational Intelligence, Security and Internet of Things*, 2020, pp. 268–279.
26. M. Vos, R. Cullen, and J. Cranefield, "RFID in the public and private sector: Key implementation considerations," 2012.
27. L. Amoore, S. Marmura, and M. B. Salter, "Smart borders and mobilities: Spaces, zones, enclosures," *Surveillance & Society*, vol. 5, no. 2, 2008.
28. S. Casiraghi and A. Calvi, "Biometric Data in the EU (Reformed) Data Protection Framework and Border Management: A Step Forward or an Unsatisfactory Move?," in *Personal Data Protection and Legal Developments in the European Union*, IGI Global, 2020, pp. 202–223.
29. S. Kloppenburg and I. Van der Ploeg, "Securing identities: Biometric technologies and the enactment of human bodily differences," *Science as Culture*, vol. 29, no. 1, pp. 57–76, 2020.
30. K. F. Olwig, K. Grünenberg, P. Møhl, and A. Simonsen, *The biometric border world: Technology, bodies and identities on the move*. Routledge, 2019.
31. B. Ajana, "Asylum, identity management and biometric control," *Journal of Refugee Studies*, vol. 26, no. 4, pp. 576–595, 2013.
32 R. Koslowski, "Smart borders, virtual borders or no borders: homeland security choices for the United States and Canada," *Law & Bus. REv. Am.*, vol. 11, p. 527, 2005.

33. D. Coardoş, E. Tîrziu, and M. Gheorghe-Moisii, “A General Framework Based On IoT Technology For Smart Governance,” presented at the 18th International Conference on Informatics in Economy, Bucharest, Romania, 2019, doi: 10.12948/ie2019.06.03.
34. D. Bigo, S. Carrera, B. Hayes, N. Hernanz, and J. Jeandesboz, “Justice and home affairs databases and a smart borders system at EU external borders: An evaluation of current and forthcoming proposals,” *CEPS Papers in Liberty and Security in Europe*, no. 52, 2012.
35. J. Jeandesboz, D. Bigo, B. Hayes, and S. Simon, “The Commission’s legislative proposals on smart borders: their feasibility and costs,” *Brussels: European Parliament, PE*, vol. 493, 2013.
36. R. Neisse, G. Baldini, G. Steri, and V. Mahieu, “Informed Consent in Internet of Things: The case study of cooperative intelligent transport systems,” presented at the 2016 23rd International Conference on Telecommunications (ICT), 2016.
37. A. Rudskoy, A. Borovkov, P. Romanov, and O. Kolosova, “Reducing global risks in the process of transition to the digital economy,” in *IOP Conference Series: Materials Science and Engineering*, 2019, vol. 497, no. 1, p. 012088.
38. M. Anouche and Y. Boumaaz, “The potential of the blockchain for coordinated border management in developing countries,” in *2020 IEEE 13th International Colloquium of Logistics and Supply Chain Management (LOGISTIQUA)*, 2020, pp. 1–7.
39. T. Yang and T. A. Pardo, “How Is Information Shared Across Boundaries?,” in *2011 44th Hawaii International Conference on System Sciences*, Jan. 2011, pp. 1–10, doi: 10.1109/HICSS.2011.226.
40. M. Janssen, P. Brous, E. Estevez, L. S. Barbosa, and T. Janowski, “Data governance: Organizing data for trustworthy Artificial Intelligence,” *Government Information Quarterly*, p. 101493, 2020.
41. P. Brous, M. Janssen, and R. Vilminko-Heikkinen, “Coordinating Decision-Making in Data Management Activities: A Systematic Review of Data Governance Principles,” in *International Conference on Electronic Government and the Information Systems Perspective*, 2016, pp. 115–125.
42. B. L. Neuby and E. Rudin, “Radio Frequency Identification: A Panacea for Governments?,” *Public Organ Rev*, vol. 8, no. 4, pp. 329–345, Dec. 2008, doi: 10.1007/s11115-008-0065-4.