

# Mobile Governance: Empowering Citizens to Promote the Rule of Law

Marta Poblet<sup>1</sup>

<sup>1</sup> ICREA, UAB Institute of Law and Technology  
Campus UAB, 08193 Bellaterra, Spain  
marta.poblet@uab.cat

**Abstract.** This paper offers an overview of the emerging domain of mobile governance as an offspring of the broader landscape of e-governance. Mobile governance initiatives have been deployed everywhere in parallel to the development of crowdsourced, open source software applications that facilitate the collection, aggregation, and dissemination of both information and data coming from different sources: citizens, organizations, public bodies, etc. Ultimately, mobile governance can be seen as a tool to promote the rule of law from a decentralized, distributed, and bottom-up perspective.

**Keywords:** governance, mobile technologies, mobile governance, rule of law

## 1 Introduction

Mobile governance is an umbrella term that covers a number of initiatives involving the use of mobile technologies (i.e. SMS, USSD, geolocation, etc.) in the domains of citizens' participation, public awareness, management of emergencies and crisis, provision of public services, information, etc. to reach wider population segments (as compared to those accessing the Internet). It is well known that mobile phones have become in recent years the most ubiquitous communication device world wide, with higher penetration rates than the Internet. In 2010, the number of mobile cellular subscriptions globally is expected to reach five billion [1]. Mobile technologies provide therefore greater opportunities for social impact than any other ICT, while being more affordable and, also, less demanding in the skills and training required [2].

While deeply intertwined to e-governance, mobile governance (or m-governance *tout court*) emerges as a new domain with two-fold objectives: on the one hand, it aims at improving the provision of basic public services, specially to the less favored populations; on the other, it bolsters the participation of citizens, grass-root organizations, NGOs, etc. in awareness campaigns, electoral processes, oversight of governments and public policy making [3]. In Hellstrom words, "mobile phones make it possible to create a bottom up participation and ultimately—what m-governance is all about—empowerment [3]. This paper presents a brief overview of this nascent domain and makes a case for considering m-governance as a crucial development of the broader domain of e-governance.

## 2 Mobile Technology for Citizens Engagement

On March 13, 2004, forty-eight hours after the terrorist attacks of March 11 in Madrid, thousands of people concentrated in front of headquarters of the Popular Party, then in office. The demonstrators wanted to know the truth on the responsibility for the attacks, the government having put the blame on the Basque terrorist organization ETA from the immediate outset. The concentration was organized in a decentralized way by means of SMS. The use of mobiles to bolster political mobilization was replicated, among other places, in the Philippines to protest against a reform on taxes (2004), in Burma during the Saffron Revolt (2007), in Iran after the election of 2009 and in several countries of Africa [4]. Mobile activism has also a significant impact on the monitoring of the electoral processes, where it can influence the way in which the elections are organized [5].

Over the last few years, new horizons and opportunities for the development of mobile governance have incredibly expanded. While the core domains of application in the area of governance are citizens' activism and public participation, monitoring of election processes, advocacy, reporting of crimes and human rights violations, new creative uses are constantly emerging. In parallel, a number of new software applications and tools have simultaneously emerged and there are teams of developers around the globe cooperating in a decentralized way to improve alpha and beta versions of the software. Among the most utilized recently are:

- *Ushahidi*—“testimony” in Swahili—is a free, open source platform that allows its users to gather distributed data via SMS, email or web and visualize it on a map or timeline.<sup>1</sup> Through Ushahidi people report real time information of events such as political disruption or natural disasters and the platform aggregates this incoming information for use in a crisis response. The website was created at the beginning of 2008 as a simple mashup, using user-generated reports and Google Maps to map reports of violence in Kenya after the post-election fallout, and it has been used in a number of election processes afterwards. But Ushahidi has really come to age with the Haiti earthquake of January 2010 with the coordination of aid and relief agencies to support rescue operations, situational awareness and near real-time online mapping of incidents related to the disaster.
- *Swift* is a free and open source toolset for crowdsourced situational awareness.<sup>2</sup> The first use of Swift was as a complement to Ushahidi to monitor the Indian 2009 Elections. Swift embraces Semantic Web open standards “such as FOAF, iCal, Dublin Core, as well as open publishing endpoints such as Freebase” to add structure to crisis data and make them shareable.<sup>3</sup>
- *RapidSMS* is an open source web-based platform for data collection, logistics coordination, and communication developed by the Innovations and Development team of UNICEF.<sup>4</sup> With the RapidSMS web interface, multiple users are able to

---

<sup>1</sup> <http://www.ushahidi.com/>

<sup>2</sup> <http://swiftapp.org/>

<sup>3</sup> <http://swiftapp.org/>

<sup>4</sup> <http://www.unicefinnovation.org/mobile-and-sms.php>

access the system simultaneously and to view incoming data as they arrive, export new data-sets, and send text messages to users.

- *Geochat* is a system of geolocated, self-organized small-group messaging over SMS. The service lets mobile phone users broadcast alerts, report on their situation, and coordinate around events as they unfold, linking field responders, headquarters, and the local community in geo-referenced conversation.<sup>5</sup>

The vast majority of these software applications are mostly SMS-based and do not necessarily need to be connected to the Internet to operate, which is a critical asset when, as is frequently the case, networks are down or shut off for either natural or political reasons (it may happen with mobile networks as well, but in this case is easier to reestablish the services or search for technical alternatives). The applications considered so far focus primarily on information gathering and sharing and on coordinating direct political actions, but less on decision making for public policies and other political deliberations [3]. The software applications have some key defining features in common, which have already been identified in recent research on crowdsourced systems: open teams, mashability, unknowable, overlapping or conflictive requirements, continuous evolution, focus on operations, sufficient correctness, unstable resources, and emergent behaviors [6].

While there is no template to design a successful mobile governance project, the literature on mobile governance has already identified some key features that seem to be present in successful case studies [7]:

- Evolutionary (vs. revolutionary)
- Embedding the mobile component into an already ongoing initiative (vs. casting the mobile service as itself the development effort or otherwise asking the technology to —lead the effort;
- Using the mobile technology to reduce transaction costs or increase productivity of existing practices, versus introducing entirely new behaviors via the mobile
- Requiring only basic literacy or skills from users, versus requiring additional technical knowledge or support

More specifically, a number of choices have been identified relating to: intended users (general public, population niches, professional groups, etc.), technical accessibility of the solution offered (i.e. low feature handsets vs. smart phones), self-contained solutions vs. links to other external platforms and services, and requirements from manufacturers or operators (i.e. cooperation with network operators on SIM cards or USSD channels, or with handset manufacturers). As Hellstrom also reminds, most projects have a strong local technological partner making it easier to manage, integrate and sustain the applications, so that the responsible body running the service hardly needs to know more than the end-user [3]. Successful m-governance applications, in sum, rely on a functioning, effective backend for content and support from a local technological partner facilitates the adoption of technologies [3].

---

<sup>5</sup> <http://www.instedd.org>

### 3 Crowdsourcing and its Effects

One of the distinctive features of the systems being currently developed is the crowdsourcing of incoming data through SMS. The notion of “crowdsourcing” was coined by Howe to describe the outsourcing of a task to “an undefined and generally large group of people in the form of an open call” [8].

Crowdsourcing data collection with mobile technologies enables faster feedback mechanisms for more informed decision-making in rapid response situations. However, it also brings new issues to the table: quality and accuracy of incoming data, validation, priority criteria, privacy of users reporting data, misuse, etc. Conversely, crowdsourcing can also be extended to the response or supply side, but then the main issues—especially in large disasters—become how to track such a distributed and decentralized response in order to effectively address the needs of the populations at risk and coordinate the relief or aid tasks [9]. The initiatives considered in this paper apply different strategies to deal with the side-effects of crowdsourcing: creating persistent identities/anonymities, tagging of incoming data, developing algorithms that filter relevant information from the noise, etc. While this may not necessarily be an issue when crowdsourcing environmental data collection (i.e. an unknown number of volunteers regularly sending reports or samples on water quality or air pollution, and then verifying those data with further test and analysis), it may raise serious concerns when the data being crowdsourced report fraud-marred elections, criminal offences, or violations of human rights in the midst of conflict events.

Crowdsourcing data collection through mobile networks holds the promise to improve decision making in emergencies, crisis and conflict events, and also to foster public participation and citizens’ awareness. But it also poses important challenges, such as accuracy (of the information provided), reliability and trust (of the multiple information sources) and, last but not least, privacy. In Shilton’s words:

At the extreme, mobile phones could become the most widespread embedded surveillance tools in history. Imagine carrying a location-aware bug, complete with a camera, accelerometer, and Bluetooth stumbling, everywhere you go. Your phone could document your comings and goings, infer your activities throughout the day, and record whom you pass on the street or who engaged you in conversation. Deployed by governments or compelled by employers, 4 billion “little brothers” could be watching you [10].

Recent examples of political violence in Myanmar, Iran or Sri Lanka have shown not only the growing citizens’ use of social media as outlets for real time reports and data on violent incidents (i.e. the use of Twitter after the 2009 Iran election) but also the exposure to government abuses when citizens use mobile networks for the same purposes. According to Martucci, ad hoc mobile networks, which “consist of computers, often mobile, that establish on demand network connections through their wireless interfaces, enabling instantaneous networking independently of the presence or aid of any central devices” [11] require the design of new privacy protocols:

Thus, most of the protocols employed in wired networks are not suitable for ad hoc networks since such protocols were designed for network environments with defined borders and highly specialized devices, such as routers, servers that provide network addresses, firewalls, and network intrusion detection systems. Moreover, such an absence of infrastructure potentially augments the risk of losing control over personal information since data is routed and forwarded through many unknown devices and users can easily be monitored. Hence, information regarding a user's communicating partners and even the contents of transmitted messages can be obtained by devices forwarding packets on the behalf of a user, if proper security measures are not implemented. Furthermore, data collection is especially not transparent in ubiquitous environments since invisible interfaces can greatly reduce the users awareness regarding when and what personal data is being collected by the ubiquitous environment [10].

While crowdsourcing offers a number of advantages to mobile governance initiatives and projects, their side-effects in terms of quality, accuracy, trust, and privacy also need to be addressed to avoid the consequences of technological misuse and subsequent risks for citizens.

## 5 Conclusion

The emerging field of mobile governance is not a substitute for e-governance. Rather, it is a complementary domain that shares the goal of providing better public services to citizens by improving access to information and data and, conversely, by opening new avenues for public participation in policy making and political debate. E-governance and m-governance share also similar concerns regarding technological choices, target populations, scalability of projects, etc. Addressing these issues and harnessing the full potential of the existing technologies available in both areas will certainly contribute to an evolutionary but sound transform of how public institutions, organizations, and citizens alike promote the rule of law on daily bases.

**Acknowledgments.** The research presented in this paper has been developed within the framework of two different projects: (i) ONTOMEDIA: Platform of Web Services for Online Mediation, Spanish Ministry of Industry, Tourism and Commerce (Plan AVANZA I+D, TSI-020501-2008, 2008-2010); (ii) ONTOMEDIA: Semantic Web, Ontologies and ODR: Platform of Web Services for Online Mediation (2009-2011), Spanish Ministry of Science and Innovation (CSO-2008-05536-SOCI).

## References

1. ITU, [http://www.itu.int/newsroom/press\\_releases/2010/06.html](http://www.itu.int/newsroom/press_releases/2010/06.html)
2. Kinkade, S., Verclas, K., Toyama, K. 2008. Reflections on MobileActive 2008 and the M4D Landscape Wireless technology for social change, [http://mobileactive.org/files/DVT\\_M4D\\_choices\\_final.pdf](http://mobileactive.org/files/DVT_M4D_choices_final.pdf)

3. Hellstrom, J. 2008. Mobile Phones for Good Governance: Challenges and Way Forward, [http://www.w3.org/2008/10/MW4D\\_WS/papers/hellstrom\\_gov.pdf](http://www.w3.org/2008/10/MW4D_WS/papers/hellstrom_gov.pdf)
4. Ekine, S. (ed.). 2010. *SMS Uprising: Mobile Activism in Africa*. Oxford: Fahamu Books.
5. Schuler, I. 2008. National Democratic Institute: SMS as a Tool in Election Observation. *Innovations*, Vol. 3 (2): 143-158.
6. Kazman, R.; Chen, H. M. 2009. The Metropolis Model: A New Logic for Development of Crowdsourced Systems. *Communications of the ACM*, Vol. 52(7): 76-84.
7. Kinkade, S., Verclas, K. 2008. Wireless Technology for Social Change: Trends in Mobile Use by NGOs, [http://mobileactive.org/files/MobilizingSocialChange\\_full.pdf](http://mobileactive.org/files/MobilizingSocialChange_full.pdf)
8. Howe, J. The rise of crowdsourcing. *Wired* 14, 6 (June 2006); <http://www.wired.com/wired/archive/14.06/crowds.html>
9. Meier, P. 2010. Using Mechanical Turk to Crowdfund Humanitarian Response. *iRevolution*, 5 February 2010, <http://irevolution.wordpress.com/2010/02/05/mechanical-turk/>
10. Shilton, K. 2009. Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection, *ACM Queue*, vol. 7(7), <http://queue.acm.org/detail.cfm?id=1597790>
11. Martucci, L. 2009. Identity and Anonymity in Ad Hoc Networks. Ph.D. diss., Karlstad University Studies 2009 (25).