# Mobile Networks and Conflict Management: Farewell to Privacy?

**Marta Poblet and Sergi Torralba**

ICREA Researcher at the UAB Institute of Law and Technology
Researcher at the UAB Institute of Law and Technology
Universitat Autònoma de Barcelona, Facultat de Dret, Campus UAB, 08193 Bellaterra, Spain
marta.poblet@uab.cat
sergi.torralba@uab.cat

**Abstract**

This paper presents a general overview of the recent rise of mobile networks and their related applications, focusing on the particular case of mobile networks and technologies applied to the early detection and management of emergencies, crisis, and conflict events. It then raises the question of how these new developments could endanger the privacy and security of their end users and briefly reviews some of the state-of-the art proposed solutions. The paper concludes by stressing the need to articulate privacy-friendly technologies to harness the full potential of mobile networks in dealing with conflict events.

## The Rise of Mobile Networks

With roughly four billion cellular subscriptions in use by 2009, mobile phones are a success story. No other technology has reached a similar penetration rate throughout the planet in a ten-year time span. Moreover, our hand-held devices are increasingly becoming mobile sensor hubs: built-in cameras, microphones, or GPS can collect images, sound, and GPS data. Tiny microscopes can be assembled to mobile phones to collect, diagnose and send geolocated images of blood samples possibly infected with malaria or tuberculosis, and then track the spread of the diseases (Breslauer *et al*. 2009). In the social sphere, the number of people who use mobile-only social networks is growing very fast. MocoSpace—a favorite in the US—Mig33—increasingly popular in Asia, Africa, and the Middle East (25 million users)—or Peperonity are among the new crop of mobile social networks (Swartz 2009). They all offer the usual social-networking tools: chat, instant messaging, photo and video sharing, etc.

In a similar way, several initiatives have been developed within the last few years with the purpose of providing accessible mobile software applications for data collection in the areas of early warning, situational awareness, emergencies and crisis response, human rights, health, or environment. Most of the initiatives come from nonprofit organizations, advocacy institutions, and relief agencies operating on the field in many developing countries in Asia, Africa, and Latin America. Some other initiatives come from international communities of researchers, such as the Information Systems for Crisis Response and Management (ISCRAM) community (Nieuwenhuis 2007). While different in scope and focus, their ultimate goal is to facilitate the collection and aggregation of crowdsourced, real-time information from local environments to support decision making in emergency situations such as disease outbreaks, natural or human-made disasters, or political events such as malpractices and violence in elections.

As a result of these nascent technologies, massive amounts of personal data will go mobile and flow over mobile networks. Without proper privacy-enhancing technologies and protocols, individuals reporting violent events or violations of human rights in hot spots could be exposed to repression and see their lives at risk. This paper addresses the need to develop privacy-friendly technologies for mobile networks to guarantee not only the protection of personal data, but also the identity and the anonymity of people supplying those data in contexts of deadly conflict. In doing so, some recent examples of mobile, open source platforms focusing on management of crisis and conflict events are presented, together with new approaches to privacy-friendly software applications for mobile networks.

## Mobile Technologies for Conflict Management

New horizons and opportunities for the prevention and management of conflicts have incredibly expanded over the last few years (Poblet 2008). A number of new software applications and tools have simultaneously emerged and there are teams of developers around the globe constantly improving them. To date, the core domains of application are health (also known as m-health), emergencies and crisis management, pollution monitoring, and citizens' reporting in election processes. 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.[1] 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.

- *Swift* is a free and open source toolset for crowdsourced situational awareness.[2] 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 (Swift, 2009).
- *RapidSMS* is an open source web-based platform for data collection, logistics coordination, and communication developed by the Innovations and Development team of UNICEF.[3] With the RapidSMS web interface, multiple users are able to 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 (InSTEDD 2009).

The vast majority of these software applications are mostly SMS-based and do not necessarily need to be connected to the Internet to operate. They 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 (Kazman and Mei 2009).

Crowdsourcing data collection through mobile networks holds the promise to improve decision making in emergencies, crisis and conflict events, but it also poses important challenges, such as accuracy (of the information provided), or reliability and trust (of the multiple information sources). Moreover, crowdsourced data also highlight what Martucci has referred to as the "identity-anonymity paradox", that is, the one "which establishes the relationship between security, identification, and anonymous communications" (Martucci 2009:33). Farewell to our privacy? The dark side of mobile networks as regards our privacy cannot be neglected. In Shilton 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 (Shilton 2009).

## Privacy-friendly software

Recent examples of political violence in Burma, 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" (Martucci 2009) 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 (Martucci 2009:2).

From this diagnosis Martucci raises the need of proper and trusted identifiers in ad hoc networks. In this regard, he establishes a connection between the lack of device identifiers and the presence of Sybil attacks and suggests

[1] http://www.ushahidi.com/
[2] http://swiftapp.org/
[3] http://www.unicefinnovation.org/mobile-and-sms.php

the use of self-certified Sybil-free pseudonyms. As for the provision of anonymous communication in ad hoc networks, he also proposes the Chameleon protocol, "an overlay mechanism that is situated in between the application and the transport layer" (Martucci 2009:33). The Chameleon protocol is said to provide "sender anonymity against recipients and relationship anonymity against local observers" (Martucci 2009:38). See also Ardagna *et al*. for a survey of existing state-of-the-art protection mechanisms and a privacy-preserving solution based on k-anonymity and multi-path communication (Ardagna *et al*. 2009).

The discussion on possible solutions to privacy and anonymity in mobile networks is heated, and it takes place simultaneously in workshops and the Internet blogs, social networks, and discussion forums. To quote one example, Nova Spivack, Twine's principal and Semantic Web expert, put in July 2009 a $10,000 challenge on how to "develop or port a technology that gives people unblockable, encrypted, anonymous Internet access for widely used mobile devices" (Spivack 2009). Among the solutions discussed within the weeks after the challenge was post, Spivack himself suggested porting the TOR platform (Anderson and Pachenko 2007) to mobile devices. Other replies proposed as an already existing solution using Bgan, a satellite Internet service,[4] combining TOR with Truecrypt for local storage data protection, or developing a web-browser accessible solution that would enable users to establish a dynamic short-range Wi-Fi mesh.

However, there is not optimal solution at this point, since each of the alternatives has its pros and its cons. The specific circumstances of each situation will determine which the main priorities in each case are: privacy, anonymity, encryption, etc.

The TOR platform can be a good option to provide some degree of anonymity to communications. The performance of TOR relies on the number of platform users: the more people use it, the better it works. The idea of TOR is to make the information flows intricate so as to obstacle the identification of the original sender. But if people are in a hostile situation and the system is no widespread enough, it might preserve the identity of the original sender, but it can also expose the other system users. Finally, if users encrypt their messages, the need of calculation power grows, and in mobile communications more quantity usually means more time delays and then, more costs.

Bgan gives a wide range of coverage by using satellites. There is no need, then, to have GSM access. Bgan may be useful when a government decides to disconnect all its population from a GSM network. Shutting down the network is relatively easy, since antennas have limited coverage, are located on the ground and can be tracked. But with Bgan this cannot easily happen, because taking control of a satellite is a far more difficult task. However, Bgan needs special hardware equipment, which may be expensive and not easily concealed. Then, in certain remote areas a person bringing such equipment could easily be considered suspicious. To minimize the costs an alternative could be having a company to own the hardware and provide the service. But, then, we face the same risks associated with the GSM network: the only thing a government needs to do is to shut down the company and its service.

Finally, the use of these technologies, thought to be used via the Internet, can severely be restricted in those countries where the main communication channels are mobile phones calls and the SMS. In addition, if messages are encrypted, most terminals would not be powerful enough to manage encryption and decryption (or a secure enough encryption).

[4] http://www.tempestcom.com

## Conclusion

Mobile networks are increasingly used for other purposes than regular phone calls or SMS messaging. Recent software developments make it possible to create mobile social networks as crowdsourced early warning or conflict management systems.

But mobile communications are easier to keep track than any other digital communication. In this context, privacy and anonymity protocols need to be tailored to fit the different requirements and architectures of mobile networks. Currently, a number of applications already offer different solutions to privacy and anonymity, but none of the existing options were originally designed for mobile networks, and then need to be adapted to this new context. Ultimately, and specially in the case of mobile networks for conflict management, users will also need to make anonymity and anticensorship everyday habits if they want to keep their privacy preserved.

## Acknowledgments

The work presented in this paper is currently developed within the framework of two parallel research 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

Andersson, C.; and Panchenko, A. 2007. Practical Anonymous Communication on the Mobile Internet Using Tor. In Third International Conference on Security and Privacy in Communications Networks (17-21):39–48. DOI:10.1109/SECCOM.2007.4550305

Ardagna C. A.; Jajodia, S.; Samarati, P.; and Stavrou, A. 2009. Privacy Preservation over Untrusted Mobile

Networks. In C. Bettini *et al*. (Eds.): *Privacy in Location-Based Applications*, LNCS 5599, 84–105.
Breslau, D. N.; Maamari, R. N.; Switz, N. A; Lam, W. A., and Fletcher, D.A. 2009. Mobile Phone Based Clinical Microscopy for Global Health Applications. PLoS ONE 4(7): e6320. DOI:10.1371/journal.pone.0006320 (accessed October 22, 2009).
Kazman, R.; and Mei, H-M. 2009. The Metropolis Model: A New Logic for Development of Crowdsourced Systems, *Communications of the ACM* 52(7), 76-84.
InSTEDD. 2009. InSTEDD Fact Sheet, May 2009. Available at http://www.insted.org (accessed June 10, 2009).
Martucci, L. 2009. Identity and Anonymity in Ad Hoc Networks. Ph.D. diss., Karlstad University Studies 2009(25).
Nieuwenhuis, K. 2007. Information Systems for Crisis Response and Management, in J. Löffler and M. Klann (Eds.) Mobile Response 2007, LNCS 4458, 1–8.
Poblet, M. 2008. Bringing a New Vision to Online Dispute Resolution. In Poblet, M. (ed.) Expanding the Horizons of ODR: Proceedings of the 5th International Workshop on Online Dispute Resolution (ODR Workshop'08). CEUR-Workshop Proceeding Series, vol. 430, pp. 1--7 (2008), http://ftp.informatik.rwth-aachen.de/Publications/CEUR-WS/Vol-430/ (accessed October 22, 2009).
Shilton, K. 2009. Four Billion Little Brothers? Privacy, Mobile Phones, and Ubiquitous Data Collection, ACM Queue, vol. 7 no.7. Available at http://queue.acm.org/detail.cfm?id=1597790 (accessed October 22, 2009).
Spivack, N. 2009. Unblockable, Anonymous, Encrypted Mobile Internet Access. Available at http://www.challengepost.com/challenge/unblockable-anonymous-encrypted-mobile-interenet-a (accessed October 22, 2009).
Swartz, J. 2009. Ads Mobilize for Social Media. *USA Today*, October 22: 8A.