Government (Officials) on the Move: The Road Ahead

Snellen, I.Th.M.

Government (Officials) on the Move

The Road Ahead

By Emeritus Professor I.Th.M Snellen

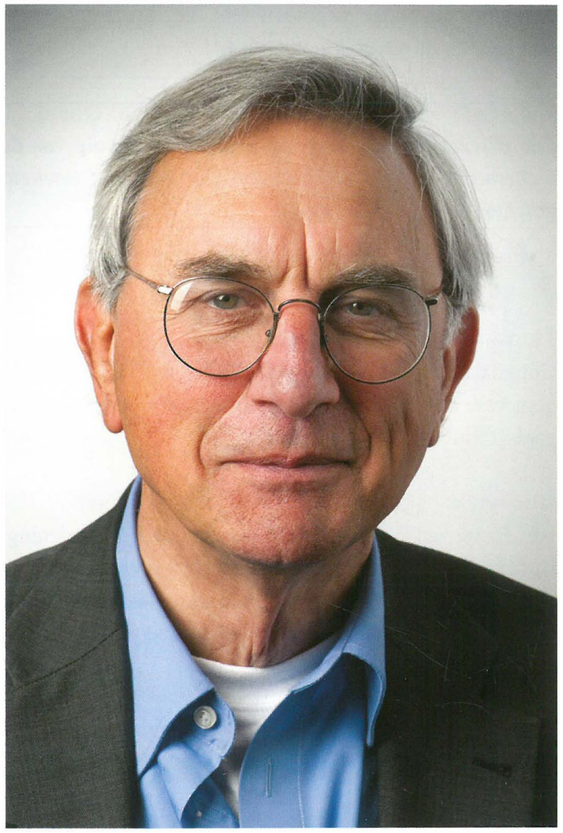
Introduction

One of the important developments taking place in the implementation of public administration today is the transition from e-government to m-government (from electronic government to mobile government). This is the application by government of mobile ICT devices such as SMS, Personal Digital Assistants, General Packet Radio Service and many more. Under the reign of e-government, the service of public administrations was adapted to citizens in such a way that mobile citizens had access to public administrations at the time and place wherever they happened to be. More recently, governments themselves are moving out of their offices, virtually or in reality, to have a closer look at the faits et gestes (actions, red.) of citizens and officials and to improve their effectiveness as well as their efficiency.

Three aspects related to the use of mobile ICTs are remarkable, and stand for the changing relationship between government (officials) and citizens through mobile ICT applications:

1. the enormously increased effectiveness, efficiency, economy, and flexibility of government capabilities through m-government applications;
2. the generally changing relationship between gov ernment and the general public through the involvement of members of the public in goverment matters;
3. the intensified control and supervision of public officials operating at street level, by higher echelons within the organization.

In this short note the question will be raised, what the influence might be of the application of mobile ICTs on the nature of the relationship between citizens and public administration. Further on it will be discussed, whether even a re-conceptualization of the relationship of the Weberian state and society has to be formulated, because of the emergence of m-government. Mobile government may inspire a more intensive service and control orientation in the relationship between the public administrative apparatus, public officials and citizens. We will also see some examples of a closer participation of citizens in the basic functions of the state, such as the assurance of the safety of the citizenry. They may be a foreboding of future relationships between state and society.



Ecology of m-government

More and more we are living in an "always on" society in which the ecology of all participants is constantly activated by a growing amount of ICT applications. This "always on" mode is also stimulated by developments that are taking place with regard to the internet. There, a recent shift can be seen that takes place from sites that rely on traditional content (providing information) to sites that focus on user generated content. This shift is often labeled as the development of Web 2.0, indicating it is a form of next generation internet. At the heart of the concept of web 2.0 lies the idea that collaborative web software makes it possible for users to work together and share information in an easy way. An important feature of Web 2.0 applications is that users are not just consumers of digital products, but, at the same time, are also active producers of digital content. Examples of typical well-known web 2.0 applications are Youtube, Wikipedia, Wikis, blogging, Hyves, Myspaces, Flickr, and Twitter.

Virtual communities arise around Web 2.0 applications and 2.0 sites. Not only for communities, but also for governments, this opens up interesting new possibilities. If citizens are seen as, and act like, active producers of digital content, as is the case in Web 2.0, then it can be interesting to think of new ways for participation of citizens in for example policy development, policy implementation, and control processes. The number and diversity of virtual communities that result from Web 2.0 applications also can strengthen the ability of citizens to stand up for themselves. They no longer have to turn to the government to solve some of their problems, but, due to the virtual communities, they are more able than before to solve them with the help of other citizens and organizations. This is made possible because Web 2.0 enables citizens to connect to other citizens and to share ideas, digital content and experiences, all in a very easy and convenient way.

Governments and officials can use Web 2.0 applications from their side to involve citizens as extensions of their administrative apparatus.

> " An important feature of Web 2.0 applications is that users are not just consumers of digital products, but, at the same time, are also active producers of digital content."

ICT support to Mobility of PA Apparatus

The apparatus of public administrations themselves are becoming more and more mobile, and are supported in this respect by mobile communication facilities, through which persons, data, objects and processes can be reached. Especially, as far as public administration is concerned, "mobile communication" offers many opportunities and challenges (Franz, 2005: 10). The following mobile applications may be mentioned:

Satellites
Modern governments position themselves even in space to utilize satellite technolo¬gies in public administration. Three functions of these technologies stand out: communication functions, earth observation functions and positioning functions.

About the author

Emeritus Professor I. Th. M. (Ignace) Snellen was born in Hilversum in 1933. He acquired a Ph.D. from the University of Amsterdam after finishing his Political Science and Law course. Em. prof. Snellen is specialised in the impact of ICT on public administration relationships. He analyses the relationships between state and society on the one hand and the relationship between public official and citizen on the other. He used to work as a Professor of Public Administration at the Universities of Tilburg, Nijmegen, Leiden and Rotterdam. He was part-time advisor Science Policy at the Dutch Ministry of Education from 1983-1986. Em. prof.Snellen is (co-) author of several scientific publications on the subject of ICT and public administration and together with W. van de Donk he edited a book entitled *Public Administration in an Information Age: A Handbook* in 1998. He also used to be President of the European Group of Public Administration (EGPA) and has worked for the Oxford Internet Institute undertaking a comparative study on the impact of internet applications.

Closed Circuit Television (CCTV)
The introduction of the first CCTV systems started in the early 1990s. The locations chosen by public administrations for surveillance cameras widely varied and were growing in amount (Webster). Through the introduction of CCTV systems, CCTV policies are entering different policy arenas, such as education, health care and transport. The capacity of the systems is growing continuously. Automatic image recognition, the automatic use of image databases, and the interconnection between systems are additions to this capacity. A recent addition is that different kinds of trespassers, discovered by CCTV, (e.g. polluting the sidewalk) are admonished by a loudspeaker to correct their behavior.

Such a surveillance of whole populations, e.g. through CCTV of all cars entering London, is becoming a rule rather than an exception. Not only are they used for road pricing, but especially in the sphere of anti-terrorism campaigns. The cameras used around London are an example of so-called "smart cameras". Through their sensors, software programs, and coupling with databases these cameras are able to register deviations of normal behavior, to alarm the control room, and/or to record this behavior. The connection of the camera with a database of e.g. stolen cars or criminals makes it possible to identify cars or suspected persons.

Radio Frequency Identifier (RFID)
Radio Frequency Identifiers use radio waves to identify products, animals, and persons. Tags or transponders are >

attached to or incorporated into the items to be identified. The identification takes place automatically and without contact of the reading device with RFID cards or with the other items, to which the tags are attached.
The uses public administrations can and will make of RFID are manifold. One can think of:

- passports and other identification documents.
- automatic road pricing and other public transport payments.
- control of food chains and supply chain management.
- fighting shop lifting and other forms of theft.
- profiling different criminals and terrorists.

Other applications are: RFID applications to follow the spread of birds' disease (Thailand), identifying information on passports (USA), patient data on tags under the skin in hospitals, which can be retrieved via a website (USA).
The tracking and tracing that is in principle possible with the help of RFID approa¬ches a completeness that makes the tendencies in the direction of supervision of total populations and advanced prevention even more pressing.

> "Citizens become eyes and ears of the public administration."

SMS criminal hunt
The SMS criminal hunt makes it possible for the police to organize a large investigation in which citizens are involved. In cases of serious crimes mass SMSs are sent from a central point to groups of volunteers and members of the police force. In this way a large investigation can be set up, and different target groups can be informed. Citizens become eyes and ears of the public administration. In more and more cities kinds of "Citizens Nets" are created to help the police in urgent investigative actions. "Nobody notices suspicious behavior better than an inhabitant of a neighbor¬hood" according to a Dutch newspaper.
Global Positioning System (GPS)
Many ICT applications provide not only content information but also an indication from which spot the information takes place. By the use of a combination of cellular technology and GPS an advanced form of local awareness in real time is created. Through this, use is being made of the reflexive power of Information and Communication Technology (S. Zuboff 1988).

ICT support to Mobile Officials

Only a relatively small portion of the officials of modern public administration are involved in policy developments. More than 70% of the public officials have a role to play in policy implementation, inspections or policy overview. These officials are called "street level bureaucrats" because they do their jobs in direct contact with citizens. As the term "street level bureaucrats" suggests, many of them do their work mainly outside the office: e.g. in police districts. Other activities of street level bureaucrats have to do with social security, labor safety inspecti¬ons, health care and health care inspections, environ¬mental inspections, etcetera. The way in which the functions of these street level bureaucrats are fulfilled is changing radically through an ever growing, amount of applications of ICT. Especially the influence of the shift from e-government to m-government deserves our attention in this respect.

General Packet Radio Service (GPRS)/Universal Mobile Telecommunication Service (UMTS)
GPRS and UMTS are techniques that are used for transferring data via mobile networks. GPRS uses the same network that is used by mobile phones. GPRS/UMTS has made it possible for the street level bureaucrat to use his mobile telephone to download data from a central database located at his "home office". He is also able to send his reports and findings as input to the central database. Direct access to a central car registration or population registration is of utmost importance. Without direct access to these registrations, the facilities to check the situation of the citizen are often completely ineffective. Special mention may also be made of the growing amount of GPRS/UMTS facilities created for tele-working in an assembly building or from home. Especially when the content of databases is being transmitted, security is still a major problem, to be worked upon.

Personal Digital Assistants (PDA)
These devices are used by mobile officials, such as police officers, who are active in neighborhoods. When they pass a coordination point that is of interest to them, the PDA will give a signal and provide information about the kind of situation that deserves their attention. It may be the address of a person free on bail, it may be a stolen car, or other situations of that kind.
The services, which are envisioned, require integration of the nervous system of public administration, through synchronization of data. E.g. the fire brigade has to be informed about relevant traffic diversions and traffic jams, as well as about permits with respect to noxious materials, logistical processes in factories, et cetera.

From Public Administration to Public Sector Control?

As far as citizens are concerned, a gradual re-definition is taking place of their role as a function within the framework of the relationship of government and society. As far as public officials (street level bureaucrats) are concerned, their activities are more and more strictly monitored and directly or indirectly controlled by "system level bureaucracies" (Bovens & Zouridis 2002) or "infocrats" (Zuurmond 1998). Protocols play an important role in this context.
Although it is often emphasized that the digital devices will lead to "empowerment" of citizens as well as public officials, we don't think this can be taken as a self-evident point of departure. The digital devices may not only strengthen the positions of citizens and public officials by making all kinds of data available at any time and any place. They are reciprocal communication devices as well, and as such they bring citizens and public officials within reach of the inspection, and of the claims of managers and others. E.g. being "absent" (not in the office, etcetera) is no longer an excuse not to be within reach, physically or virtually.

> "Being 'absent' (not in the office, etcetera) is no longer an excuse not to be within reach, physically or virtually."

Growing Public Functions of Citizenship?
In a recent publication, the Dutch Rathenau Institute, an independent technology assessment organization, has published a study entitled: "From Privacy Paradise to Control State". With respect to the intelligence and security measures which are being created in the wake of the fight against crime and terrorism, it distinguishes the following trends:

1. Intelligence gathering is increasingly extending to people, who are not suspects, but who are part of the suspect's environment.
2. The research is increasingly adopting an explora tory character, in which potentially suspect groups are being monitored on the basis of risk profiles.
3. Legal restrictions on the use of certain detection methods are being eased or lifted.
4. Intelligence services are acquiring more and more opportunities, both legal and technical, to carry out (independent) investigations.
5. Intelligence services increasingly have access to information from other government and semi-privatized services that has been collected for purposes other than intelligence.
6. Intelligence services are increasingly forcing other parties to cooperate in investigati¬ons (Vedder e.a.).

> "Intelligence gathering is increasingly extending to people, who are not suspects, but who are part of the suspect's environment."

These trends, observed by the Rathenau Institute, are not only important as such, but they are a matter of concern for many people. They represent the kind of changes that is implicated in the transition from e-government to m-government. They also bring forward the question whether, and to what extent, the relations¬hip between state and society, or between public administration and citizen, is chan¬ging more fundamentally.

Re-defining the Weberian State-Society Relationship?

According to the generally accepted definition of the state, developed by the German sociologist, Max Weber, a state is "a geographically delimited segment of human society united by common obedience to a single sovereign". In this definition three essential elements of a state are distinguished:

1. the territorial basis of the state;
2. the population living within the confines of this territory;
3. the paramount control and ultimate power of the state. >

Since the massive introduction of Information and Communication Technological applications in state and society, the physical, demographic and jurisdictional boundaries of the modern state have been shifting.

The *territorial* basis of public administrations is affected by the installment of tracking, tracing and monitoring applications, such as Global Positioning Systems (GPS), put in orbit, through which all kinds of activities and developments on earth can be supervised.

The *demographic* basis of the state administration - at least in the Western world - is affected by a massive influx and outflow of, on one hand, asylum seekers and economically motivated immigrants and cross border workers, and on the other hand sun seeking pensioners.

The *jurisdictional* basis of the state – its paramount control and ultimate power basis – is affected by the globalizing developments in the world. Some of the side-effects of globalization are a growing-border crossing international criminality and terrorism, tax-evasion, traffic in women, etcetera. The jurisdictional limitations that nation states encounter when they fight the negative effects of a globalizing world are putting them under more and more pressure.

Conclusions

In 1998 the Dutch Scientific Council for Government Policy, the most important scientific advisory council of the Dutch government, published a report entitled "State without Country". The report focused especially on how the consequences affect the state's power to act. Modern state administrations are, in their essential dimensions, becoming "mobile state administrations" themselves.
Their territorial basis has been extended into virtual directions, their demographic basis
has become extended and more diversified, and their jurisdictional basis has only partly been strengthened by the still growing transparency in the relationships between state and society.
A more systematic study of the interrelationships between changes from e-government to m-government within countries, with changes in the role relationships of public officials and citizens, and with changes in state society relations, deserves our attention.

> "Modern state administrations are, in their essential dimensions, becoming 'mobile state administrations' themselves."

At the start of this paper the question raised was: does the deployment of mobile ICTs lead to fundamental changes? In the end of the paper the question was raised whether a re-conceptualization of the Weberian state–society relationship has to be considered.
The answers we found on these questions relate in the first place to the policy implementation aspects of public administration. The fundamental shifts we notice in these aspects is a growing functionalization of the role of citizens in the state society relationship, on one hand, and a growing infocratization (Zuurmond 1998) of the position of the street level bureaucrat on the other. Although these observations are based on quite recent developments, they point in a direction that has to be taken seriously.

The Weberian state society relationship is changing fundamentally as well. Governments are on the move outside their age honored geographical, demographic and jurisdictional boundaries. They are becoming more and more footloose. Those physical boundaries of the state are more and more replaced by virtual boundaries. This cannot remain without consequences for the quintessential dimensions of the state. ■

References

Franz, A. (2005), Mobile Kommunikation: Anwendungsbereiche und Implikationen für die Offentliche Verwaltung, Speyer.

Kaneko, Y. (2005), The Use of Space Technologies for More Effective and Efficient Public Administration, in: Petroni, G. and F. Cloete, New Technologies in Public Administration, IOS Press, Amsterdam, pp. 90-104.

Vedder et al.(2007) Van privacyparadijs tot controlestaat, Rathenau Institute, Den Haag.

Webster C.W.R. (1996) Closed Circuit Television and Governance: The Eve of a Surveillance Age. In: Information Infrastructure and Policy, vol.5, nr. 4 pp 253-63

WRR (Scientific Council for Government Policy) (1998). Staat zonder Land (State without Country)

Zuurmond A. (1994) De Infocratie. Een theoretische en empirische herorientatie op Webers ideaaltype. (The Infocracy. A theoretical and empirical re-orientation on Weber's ideal-type.) Rotterdam Phaedrus

Cyberwar en de risico's van de digitale overheid

door Tom Degen

Binnen het openbaar bestuur neemt ICT een steeds grotere rol in en zij draagt daarmee bij aan de ontwikkeling van de informatiesamenleving. Nieuwe ICT-ontwikkelingen hebben telkens gevolgen voor de wijze waarop de overheid in de samenleving kan opereren. Hierdoor kan ICT ingrijpende veranderingen veroorzaken in de relatie tussen de overheid en burgers, bedrijven en maatschappelijke organisaties. Dit gebeurt doordat ICT nu al in alle primaire processen van de overheid betrokken raakt, zoals bij beleidsvorming, handhaving, toezicht en ook steeds meer in de democratische functie (Lips et. al, 2005). De overheid gebruikt ICT verder om data van burgers, bedrijven en haar eigen handelen op te slaan. Hiermee tracht zij efficiënter en effectiever te werken. Het openbaar bestuur verwordt zo tot een digitaal bestuur. De meeste aandacht gaat uit naar de mogelijkheden die ICT voor de overheid met zich meebrengt. De vraag wat de risico's zijn van deze digitalisering blijft vaak achterwege. In dit artikel zal ik ingaan op deze vraag. Eerst zal ik de achtergrond schetsen, vervolgens de risico's benoemen en tot slot de oplossingen en uitdagingen voor overheden formuleren.

De vervlechting van ICT als onderdeel van de verandering naar een informatiesamenleving heeft ervoor gezorgd dat de overheid en de samenleving steeds afhankelijker zijn geworden van informatiesystemen, datasystemen en digitale netwerken. De risico's van gepubliceerde informatie op internet zijn duidelijk te zien in de Cablegate affaire, waarbij vertrouwelijke documenten van de Amerikaanse diplomatieke dienst in de handen zijn gekomen van WikiLeaks. Niet de inhoudelijke onthullingen in deze documenten, maar het feit dát deze informatie ter beschikking staat van een onbereikbaar extern netwerk is het meest interessante aspect aan deze kwestie. Het laat de onmacht zien van de staat om dergelijke informatieverspreiding tegen te gaan wanneer internetgebruikers op collectieve en individuele basis de informatie verspreiden en beschermen. Acties van verschillende overheden om verspreiding tegen te gaan, leidden tot cyberaanvallen op de websites van Mastercard, Paypal, en ook het Openbaar Ministerie in Nederland. Globalisering en de netwerksamenleving hebben er toe geleid dat er serieuze zorgen zijn over de mogelijkheden van overheden om data, informatie en processen te beveiligen. De Cablegate affaire lijkt deze zorgen opnieuw onder de aandacht te brengen.
De aandacht voor en bezorgdheid over cyberveiligheid onder burgers en media is een ontwikkeling die al langer speelt (Cornish et al., 2010). Overheden en internationale organisaties focussen zich steeds meer op deze nieuwe dreiging. Zo hebben het Verenigd Koninkrijk en de Verenigde Staten aangekondigd fors te investeren in cyberbeveiliging en heeft de NAVO een Cyber Security Centre of Excellence in Tallinn opgezet. De keuze om dit centrum in Estland te vestigen, heeft deels een symbolisch karakter. In 2008 werden overheidssites en netwerken van Estland vanuit Rusland geïnfiltreerd en platgelegd. Dit wordt gezien als één van de eerste cyber-aanvallen in een nieuwe dimensie van cyber-oorlog (Buckland et al., 2010). In juni 2010 werd de Stuxnet-worm via USB-sticks verspreid naar computers wereldwijd. Dit virus was dermate complex dat er wordt gesuggereerd dat het alleen door overheid gesteund werk kan betreffen. Het was ontworpen om een specifiek industrieel controlesysteem te infecteren en daarmee een bepaalde installatie te onderbreken. Gezien het feit dat de uitbraak geconcentreerd was in Iran, lijkt het erop dat de nucleaire faciliteiten het doelwit waren. De Verenigde Staten en Israël zijn potentiële daders. "This, it seems, is what cyber war looks like. Get used to it." was het commentaar van The Economist (2010). Bij dergelijke cyberaanvallen is de dader vaak onbekend, gezien deze virtueel en vaak anoniem handelt. Het is daardoor lastig om te onderscheiden welke acties daadwerkelijk een aanvallend karakter hebben en welke voornamelijk criminele activiteiten ontplooien. De nieuwe dreigingen die het digitale netwerk meebrengen zijn: cyberaanvallen gesteund door of uitgevoerd vanuit een staat, extremisme (vaak cyberterrorisme genoemd), georganiseerde criminaliteit en individuele criminaliteit (Cornish et.. al., 2010).

Deze dreigingen zorgen ervoor dat verschillende overheden fors investeren in cyberdefensie. Zo investeert de Amerikaanse overheid de komende vijf jaar al 50 miljard dollar in haar cyberdefensie. Op dit moment wordt het globale netwerk van het Amerikaanse ministerie van Defensie wereldwijd miljoenen keren per dag aangevallen en in de toekomst zal dit naar verwachting alleen maar toenemen. Dit alles terwijl de rol van cybertechnologie binnen het defensieapparaat al aanzienlijk is. Cybertechnologie is gedurende conflictsituaties van essentieel belang omdat wapensystemen, satellieten en communicatienetwerken allen afhankelijk zijn van deze technologie.
Doordat het aantal gebruikers ieder jaar met tientallen miljoenen toeneemt, zal het globale netwerk steeds >

> "This, it seems, is what cyber war looks like. Get used to it."