# 10 Everyware

You walk into the [the conference room, living room, museum gallery, hospital ward], the contextual intention system recognizes you by your [beacon, tage, badge, face, gait], and the [lights, music, temperature, privacy settings, security permission] adjust smoothly to your preferences. Your new location is announced to the [room, building, global buddy list, Homeland Security Department], and your [video conference, favourite TV show, appointment calendar, breakfast order] is automatically started.

—Gene Becker

Now, nothing need be without processing power, and nothing need be left unlinked. . . . Networked intelligence is being embedded everywhere, in every kind of physical system. Code is mobile. Code is everywhere.

—William J. Mitchell

At stake is how the destabilization of time and space by data-intensive environments will be interpreted and employed: as time and space become more malleable, will this flexibility be used to enhance and amplify human life, or to drive humanity closer to thinghood?

—N. Katharine Hayles

The last three chapters have explored, in some detail, how software is increasingly being embedded in objects and space and enrolled in a range of practices with diverse implications. Given the trends outlined, it is easy to conclude that Western societies are advancing toward a situation in which code is routinely employed to undertake tasks and solve problems across all aspects of everyday life. This broad use of code is being actively explored by a wide range of computer scientists, new media designers, technology analysts, and IT corporations keen to explore such a scenario. The outcomes sought are to advance technical understandings and conceptual thought; produce prototype systems; and to exploit new commercial opportunities. These ideas are driven by the idea that rather than always taking work to the computer, computation should be available wherever it is needed; computation should be organized around people and their everyday lives, and not human lives around computation, as

is presently the case (Dourish 2001). The new paradigm they are seeking to introduce has been termed "everyware" (Greenfield 2006).

Everyware is the notion that computational power will soon be distributed and available at any point on the planet—calculative capacity will be literally available everywhere, with multiple computers operating for every person. Many everyday objects will become computational devices and be promiscuously networked as microservers that are continuously accessible across an Internet of things, unobtrusively chatting to each other about small but significant matters. In other words, everyware is a state in which computation can be continuously on-hand, regardless of location, and thoroughly interwoven into the fabric of society. With everyware, life unfolds enveloped within software-enabled environments (Mitchell 2004). Software will become truly hospitable to social life, and the type of computers we have lived with for last two decades will disappear from view.

It is apparent that nascent forms of everyware already exist, at least for some people, and in some parts of the world. Much of the West is saturated with software-enabled, networked technologies supported by fixed line and wireless infrastructures (near field and proximate communication with Bluetooth, local Wi-Fi coverage, national GSM/3G networks, satellite connectivity); nations such as Finland are approaching 100 percent cell phone penetration (OECD 2008). Many daily practices are overdetermined by code. With access to the appropriate technology, it is possible to connect to ICT networks from anywhere on the planet. However, everyware in its contemporary deployment is highly partial in nature, uneven, and unequal in distribution, density, penetration, sophistication, and form. Access is dependent upon economic resources, knowledge to use technologies, location, and whether appropriate infrastructure is available, and devices and networks being interoperable. Computer and network usage is constrained by social conventions, cultural differences, language barriers, and legislative mandates; the freedom of access is also subject to surveillance, censorship, and control by the state and corporations (RSF 2008).

In this chapter, we detail how advances in different forms of computing, pervasive, ubiquitous, sentient, tangible, and wearable, are creating the technologies and infrastructures to make everyware a reality. We then examine three discursive regimes that are driving the development of everyware—empowerment (convenience, utility, productivity, play, military enhancement), securitization (surveillance, discipline, crime preclusion, risk reduction), and sousveillance (the personal monitoring and management of one's life, as opposed to endogenous surveillance that seeks to control; Mann, Nolan, and Wellman 2003). In the second half of the chapter, we examine why we believe everyware will always remain partial in nature, focusing on the desire of people to adopt core technologies, the persistence of gaps in the production and deployment of everyware, and how people already avoid and resist software-enabled technologies and will continue to do so for a number of reasons.

## Defining Everyware

Following Greenfield (2006), we conceive of *everyware* as an umbrella term that encompasses a range of related forms of computing and social software that are often used synonymously, including: pervasive, ubiquitous, sentient, tangible, and wearable computing and ambient intelligence. These forms of software interaction are linked through the shared aim of opening up computation to everyday tasks, rather than tailoring a task to fit the constraints of current computer interfaces. Moreover, many tasks, it is envisioned, will be performed automatically such that people are not aware that software was active in the solution. There are, however, some subtle differences as to what these various forms of computing constitute, despite the fact that the terms are often used interchangeably and the forms of computing are used in conjunction with each other.

Pervasive computing seeks to augment aspects of everyday life and activities by adding value through the embedding of sensors and some degree of decision-making capacity in everyday objects and infrastructures rendering them interactive and smart, yet also mundane and routine. As we have detailed throughout this book, code is now being embedded into all manner of objects, very few of which present themselves as computers (see chapter 3). By 2005, less than a quarter of the microprocessors made by Intel were for desktop and laptop computers. The overall aim of pervasive computing is to ensure that an individual can interact naturally with and within an environment as opposed to operating a single digital device; tasks would be automatically coordinated, distributed, and shared across multiple devices where there is no one point of control (Dourish 2001). Over time it is hoped that systems will not only adapt themselves to their users, but that they will observe, learn, and, in some sense, be able anticipate the user's needs (Aarts, Harwig, and Schuurmans 2002). Successful pervasive computing, for Weiser (1991, 3), weaves itself "into the fabric of everyday life until they are indistinguishable from it." As such, processing power becomes so pervasive in environments that computers per se effectively disappear. This is the mission of projects such as MIT's Project Oxygen:

> We will not need to carry our own devices around with us. Instead, configurable generic devices, either handheld or embedded in the environment, will bring computation to us, whenever we need it and wherever we might be. As we interact with these "anonymous" devices, they will adopt our information personalities. They will respect our desires for privacy and security. We won't have to type, click, or learn new computer jargon. (www.oxygen.lcs.mit.edu/Overview.html, January 15, 2009)

As this quote illustrates, interaction is facilitated by sentient and tangible computing. Sentient computing is where objects and systems sense and react in a contextual fashion to an individual's presence, without having to be asked or directly instructed

(Addlesee et al. 2001). The opening quote of the chapter provides several examples of sentient computing—wherein an individual is automatically recognized and depending on circumstance and context, the software reacts appropriately (for example, opening a door lock, increasing the thermostat temperature, showing datebook appointments). Other kinds of sentient computing include occasions when peripheral devices, such as networked printers and data projectors, make themselves known to codejects that come into their wireless network and react accordingly; or toys that know they have been picked up or interacted with in some way and react in a contextual fashion to the nature of play. It is thus argued that sentient computing allows people to personalize their network appliances so that environments know who they are and what they have done in the past, and can consequently react to them in ways that are appropriate or helpful.

Tangible computing, on the other hand, is an individual controlling computation, but in a manner that employs more natural modes of communication such as voice and gesture recognition and touch, rather than being statically positioned in front of a screen and typing at a keyboard or clicking a mouse—modes of interaction that have varied little since the invention of the digital computer (Dourish 2001). Indeed, in many ways, computers remain hard to use for many simple tasks. The aim of tangible interfaces is to make interaction with software into a normal, natural, tacit practice; something much less cognitively taxing and intimidating, thoroughly intuitively usable, and little different from conversing with a person. In this sense, everyware should be a "calming technology," as envisioned by Weiser and Seely Brown (1998). As Dourish (2001) notes, thinking about and developing these more intuitively humanistic modes of interaction with software requires moving from fixed hardware input devices and constrained metaphorical ideas, such as desktops, folders, and menus to ideas centered on the ways people "naturally" experience and engage with the world through voice, embodied gestures, and innate touch. All manner of objects and surfaces will receive digital inputs and give outputs; other digital objects will operate touch free. Recent innovations in touch screens and interface designs, as exemplified by Apple's iPods and iPhones, provide some hints toward the much more intimate interaction that tangible computing promises, but natural speech interfaces, long held as the apogee of human-computer interaction, are still presently in their infancy.

Whereas pervasive computing is software capacity embedded in environments that then interact with people moving around within them, ubiquitous computing is computation power that moves with the person regardless of environment. As such, ubiquitous computing refers to coded objects that people carry or wear that can solve tasks as they move about, or will react automatically and appropriately to changing environments and activities, depending on communications with local informational resources and infrastructural networks. Pervasive computing exhibits processes of divergence—software being embedded into more and more devices—whereas ubiqui-

tous computing exhibits convergence, with single coded objects undertaking more and more tasks (see figure 10.1). While pervasive computing needs to be situationally aware to be successfully implemented, ubiquitous computing requires continuous context and location awareness. It is hypothesized that in time, how a coded object behaves will vary seamlessly with where one is, who one is with, and what one is doing (Greenfield 2006). A obvious example would be cell phones that would ring audibly only when it was appropriate to do so (this is simple for people to judge but actually hard to program algorithmically).

Wearable computing is where software migrates from specific coded objects to become embedded into the clothes, shoes, jewelry, and accessories that are commonly worn. The fibers and fabrics of clothes and accessories gain digital functionality, some awareness, and become programmable to a certain degree; they can identify and sense the person wearing them and something of the environment around them; they can potentially communicate with other wearable devices and coded infrastructures; and they can act as interfaces to other devices (Mitchell 2004). An early example would be a digital hearing aid, but envisaged examples include a shirtsleeve used to interface with an iPod (brushing down to decrease volume, up to increase volume, tapping to start and stop tracks); a jacket that could keep its wearer warmer in cold weather or change color on demand; shoes and socks might tighten and stiffen to alter gait and prevent injuries. In addition, the clothes and accessories might also automatically record where they go and who they encounter, monitor vital signs, and contain conductive fibers that can generate their own electrical power from body heat or movement (Andrejevic 2007). Mann (1998) suggests that genuine wearable computing can be characterized by the following qualities:

*Unmonopolizing* It does not demand full attention.
*Unrestrictive* Other tasks can be completed while using it.
*Observable* The wearer is aware of its work.
*Controllable* It is responsive and the wearer can take control of the process at any time.
*Attentive* It has some awareness of the situation and/or environment around it.
*Communicative* It can communicate with other devices and express the wearer's desires.
*Constant* It is always on and ready to solve tasks.
*Personal* It becomes prosthetic-like in its use (it becomes an unthinking extension of the body); it is private to the individual wearer.

If the mantra of pervasive computing is computation in every thing, then the mantra of ubiquitous computing is computation in every place. Ubiquitous computing requires, on the one hand, the development of much more effective mobile devices and, on the other, a rollout of universal networking coverage so that interactive com-

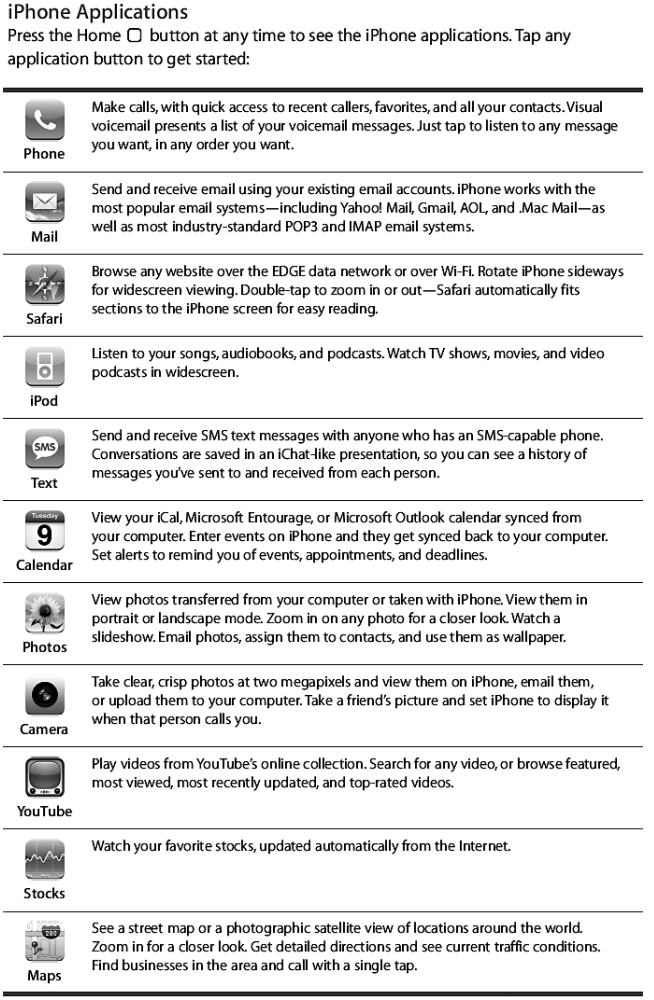



**Figure 10.1**

Apple's iPhone, at the vanguard of cell phone technology, is a single coded object with software to solve tasks of telecommunication, Web browsing, personal organization, taking a picture, and serving as an MP3 player and a game device. Code can offer multiple functions in a single object. This computer is, in a profound sense, the universal machine.

munications can occur regardless of any particular location. Clearly, there have been significant strides made in both of these areas in the last two decades with the development of increasingly sophisticated handheld, mobile, multifunctional devices, such as hybrid phone/PDAs and the rollout of GSM/3G telephony and wireless Internet broadband in many countries (see figure 10.2). However, a key constraint with ubiquitous computing, based on mobile devices, is the availability of electrical power and the limited life of batteries (see figure 10.3).

Conceptually, it is possible to imagine the interlinking of all of these forms of computing because, as Greenfield (2006, 97) notes, "everything digital can by its very nature can be yoked together." After all, at a fundamental level, they all they share a universal language—zeros and ones. That is not to say that such convergence is practically possible or desirable—after all, at present and for the foreseeable future, coded objects, infrastructures, and processes use different capta formats, incompatible standards, inconsistent protocols, and a raft of legal barriers and political economy constraints.

Taken together, it is envisioned that these various forms of everyware will generate "ambient intelligence"—objects and spaces that are sensitive and responsive to the presence of people or other coded objects. Such ambient intelligence is defined by being context aware (a space recognizing the people occupying it and understanding sufficient aspects of the ongoing context), personalized (a space that can be effortlessly tailored to the desires of the occupier), adaptive (a space that changes automatically in response to the actions of the occupier and the unfolding situational context), and anticipatory (a space that predicts likely future desires based on prior interaction and unfolding context) (Greenfield 2006). In this sense, everyware is driven by adaptive software—code that is self-organizing and self-learning. It is not intelligent in the classical sense of producing devices and environments that have consciousness, and can socialize on some higher level with people, but smart in that it is aware and responsive. As Sterling (2002) notes, people want to be facilitated, but no one wants to be bossed around by algorithms.

All of the forms of novel computing we have outlined so far are in the process of being explored by university labs and corporate research centers, and some have made it to market in various guises. While prototypes are often rudimentary when compared to end visions of everyware, they nonetheless point to what is possible and the likely trajectories of development. Indeed, all ten of the essential characteristics of everyware detailed by McCullough (2004) presently exist to some extent, as we have illustrated in a range of contexts and practices in the previous three chapters.

- Space and objects are embedded with software functionality.
- Sensors detect some kind of action and generate capta that represents it.
- Communication links form an ad hoc ecology of coded objects.

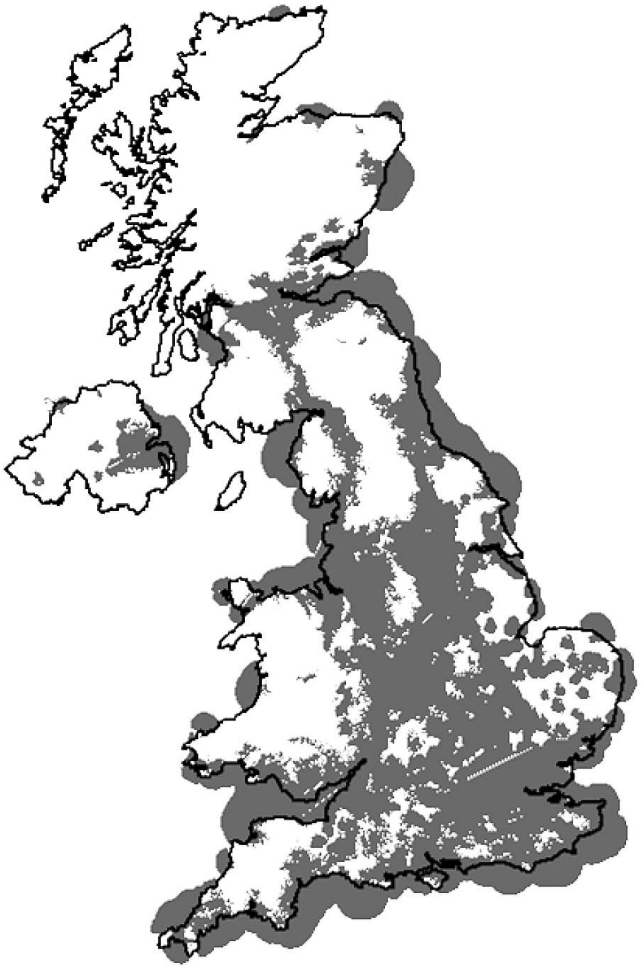


**Figure 10.2**
The extensive 3G wireless coverage provided by Orange network in the UK at the end of 2008. Despite the apparent gaps for some rural areas, the majority of consumers have access. *Source*: Ofcom 2009, www.ofcom.org.uk/radiocomms/


**Figure 10.3**
A creative business solution to overcome battery constraints. A street charging-service provider in Kampala, Uganda. *Source*: Jan Chipchase 2006, www.janchipchase.com/sharedphoneuse

- Tags identify actors.
- Actuators close the loop (a system regulates itself by monitoring its own performance).
- Controls make it participatory (a system you interact with rather than react to).
- Display spreads out (interfaces becoming more ubiquitous).
- Fixed sensor grids can track mobile positions.
- Software models situations.
- Tuning and adaptability overcomes rigidity.

The development and diffusion of everyware then appears to be inevitable in the long term, although the exact form is impossible to predict. Indeed, some spaces are already prototypical everyware environments such as airports and many other significant coded assemblages. However, it should be noted that everyware is developing differently between locations (McCullough 2004; Greenfield 2006). For example, in Japan the trend has been toward ubiquitous computing primarily using cell phones (Greenfield 2006). In North America, the trend is toward pervasive computing and the

embedding of code into environments. One of the most ambitious rollouts of a proto-everyware environment at present is the conceptualization, design, and development of Songdo City, forty miles from Seoul, South Korea (see figure 10.4). This new city, built on a green field site, is conceived as a "ubiquitous city," thoroughly infused with software technology where "all major information systems (residential, medical, business, etc.) share data; computers are built into the houses, streets and office buildings; and the technology and facilities infrastructures are integrated and pervasive" (Songdo 2009a). The developers' aim is that the people who live and work in Songdo "will experience an unparalleled Quality of Life as technology, resources and innovation all come together to create the ideal environment" (Songdo 2009b).

## The Drivers of Everyware

. . . will ubiquitous computing be co-opted as a stalking horse for predatory capitalism or can we seize the opportunity to use it for life-enhancing transformation?

—N. Katharine Hayles

As we detailed earlier in the book, the embedding of software into everyday life is supported by a powerful discursive regime consisting of sets of interlocking discourses relating to efficiency, productivity, safety, sustainability, and consumer choice. It seems to us that the drive to develop the conditions of everyware draws on these

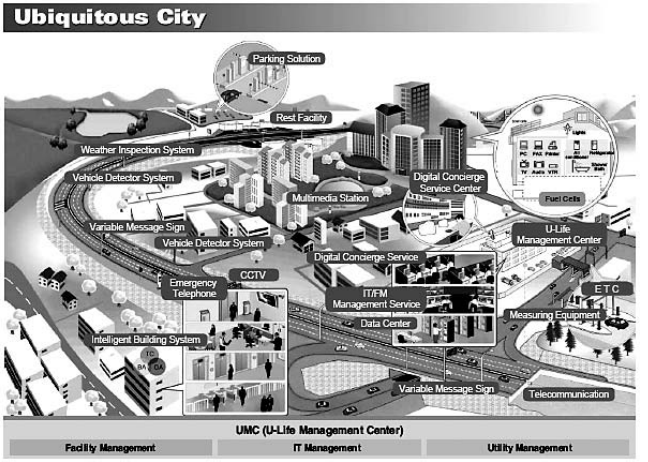



**Figure 10.4**
Songdo City, a self-styled ubiquitous city in the making. *Source*: www.korea.net/korea/view.asp?murl=/image/news/today/

discourses, but more particularly those relating to empowerment, securitization, and sousveillance. Everyware offers a future that enables and empowers individuals on the one hand, but can also greatly augment the capacity of states and corporations on the other.

### Empowerment through Everyware

As we discussed in chapter 6, software affords its users a mechanism and media for creativity, and empowers them to do new kinds of work in the world. Software helps people solve relational problems in a more effective, cost-efficient, and innovative way. The central premise of much everyware is to take the affordances that software makes to people's lives to a qualitatively higher level. The calculative capacity of code will become instilled deeply into all aspects of everyday lives in order to enhance enjoyment and productivity and also empower people in diverse ways, as the opening quote below illustrates. In this section, we examine in brief some of the forms of everyware being envisioned and developed by technologists that potential to empower people.

*An individual is walking down a street in a U.S. city in the near future. A Bluetooth-enabled jacket relays music wirelessly from a multipurpose device in a pocket to the person's earphones. The controls of the music player are embedded in the jacket's fabric. A pair of ordinary-looking eyeglasses is wirelessly connected to the same device, providing an augmented reality overlay on the environment being navigated, supplying contextual information about the buildings being passed or the route to be taken. The system software notes from historical capta that this is the fourth time this month that the person has walked down this street, while it also logs ambient noise levels and air temperature. By tapping on a sleeve, the device can be used to query specific information requests, such as looking at a restaurant's menu and making a reservation for later that day. Sitting on a bench, the glasses can be tuned to watch television, play a movie, or browse the Web. Also built into the glasses is a lens and CCD sensor that allows them to mediate reality, enhancing what the wearer is viewing by projecting a high resolution image onto the lens of the glasses, perhaps enlarging text or allowing the person to zoom in on a faraway scene. The glasses could also be connected to a captabase of people previously met, or a centralized store of capta, that is enabled by face-recognition software, so as to identify the people in vision and to provide subliminal or explicit cues on who the person is and how to act. Sensors and actuators in shoes react to foot form, terrain, and walking or running speed to absorb the most impact and support joints. A wristwatch not only tells the time but measures pulse, body heat, and blood pressure to monitor stress levels, all of which is logged and stored in a compressed form. Bluetooth enabled, it will also communicate with a cell phone to display text messages.*

*The individual arrives at home. The house's coordinating software system recognizes the person remotely from an identity tag (such as an RFID) and after a quick authenticating fingerprint scan on the door handle, it is automatically unlocked and opens. The time of the door being unlocked and who enters is logged. On entering the house, the lights come on as necessary and a small mirror display in the hallway subtly indicates the presence of other family members in the dwelling, their location, and their activity. As the person walks into the kitchen, a wall surface acts as a screen displaying any new messages. The person places a meal into the microwave, and the 2D bar code communicates to the machine the optimal cook settings. The person loads dirty laundry into the washing machine, and the RFID labels on the clothes inform the machine of the appropriate wash cycle. The person verbally tells the house's coordinating software systems that they will want to take a bath shortly at the usual temperature setting. Next, the person deals with messages. To add the contact of a potential client from that afternoon to the person's address book, the prospect's business card is placed next to the screen and the details are transferred electronically and stored for future use.*

This kind of scenario aims to make people information rich and able to make more informed decisions. While such scenes were very much science fiction a couple of decades ago, they are now actively being developed and prototyped. For example, companies are already developing wearable computing. Burton and Motorola were selling Bluetooth enabled jackets in 2004–2005, and Adidas marketed a running shoe that would respond to the runner's biomechanics (Greenfield 2006). Several university research labs, such as the MIT Media Lab, ePi Lab Toronto, Wearable Computing Oregon, and IfE Zurich, are working on prototype smart clothing, watches, accessories, and video enabled glasses. Much work has focused on military applications designed to improve the performance of soldiers and their safety. For example, the development of voice-activated, heads-up displays attached to helmets that can map overlays, including the real-time location of comrades, images from a camera mounted to a gun (that enables the soldier to see and fire round a corner without visibly exposing the body), and the results of face recognition processing of people at checkpoints, built-in communication devices, digital cameras, and GPS, as part of modular wearable computers that enable soldiers hands-free access to data and video (Rensing et al. 2002; Page 2007; Crane 2008). To date, companies such as Xybernaut, CDI, and ViA Inc. have tried to develop more mainstream commercial applications, but so far they have largely failed. Indeed, one must be wary of the exaggerated claims of the weapons industry surrounding the potential of techno-warriors and the role of code to somehow sanitize the embodied practice of killing on the battlefield (Graham 2007).

As detailed in chapter 8, companies and research labs are also seeking to envision and build the homes of the future. The goal, as with much previous domestic technol-

ogy, is to increase convenience by delegating more components of routine tasks to machines. In most cases, software is used to enhance the functionality of domestic appliances and to ensure they work appropriately without explicit instruction from a human. In effect, the home is envisioned with a set of smart networked peripherals.

Other researchers in university labs and commercial companies are seeking to bring location-based services (LBS) to the mass market, building on the success of personal satnav systems provided by companies such as Garmin, NavTeq, and TomTom. Morville (2005) characterizes GPS navigation as Wayfinding 2.0—navigation that extends beyond human memory or analog aids by tracking in real time the path taken while providing person-centered directions to a location. LBS adds significantly more capta to the system by enabling the mapped environment to act as a geographical interface to spatially relevant information about that environment. For example, by clicking on part of the map that represents a particular feature—such as a town or a building—contextual information regarding that place can be offered and locationally relevant responses and feedback given. Querying a train station would list the services leaving and arriving over the next couple of hours; querying a museum would provide details about the current exhibition, opening times, and admission charges; looking at a store could link to its online catalog. LBS envelops people within an "ambient findability," wherein the environment surrounding them is rendered transparent to enquiry and interaction—a world in which we can find anyone or anything from anywhere at anytime (Morville 2005). (Note, this of course resonates with deep-seated modernist fantasies of the individual being able to make the world into an ordered and knowable place working in service of their need.) In effect, software enables navigating the world to become a means of navigating information.

It is envisioned that consumers will be empowered by everyware technologies through the provision of richer information concerning the products that they buy. As detailed in chapters 4 and 9, it is projected that consumers will be able to easily query the ingredients or components of a consumer good, examine their history, the conditions under which the product was manufactured, or its capacity to be recycled (see chapter 11). In addition, it will be trivial to track and trace the use and location of things owned. For example, a mislaid pen could be easily located, queried as to when it was bought, how much it cost, the name of the pen design, and how much ink is left. Clearly this is useful to a certain degree, but also introduces unnecessary and largely redundant surveillance.

There are many other potentially socially productive applications of everyware for individuals and communities. For example, with respect to environmental monitoring, networks of sensors will be able to monitor different land-based ecosystems, the oceans, and the atmosphere, and relay information in real time about their status (Butler 2006). This kind of information might have a positive effect on communal consciousness about resources, and could aid democratic decision making (Dennis

2008). We can also envision a network of sensors in hospitals or homes that constantly scan the air, surfaces, water, and food for germs, viruses, and contagious diseases and various forms of pollution, with automated software analysis that can alert people when pathogens are detected or when thresholds are exceeded. For example, water faucets might scan and test the quality of the water supply as the water flows through them, alerting users if there is a problem; this clearly plays on the common discourses of hygiene and contamination that are entrenched in social psychology, along with more consumerist desire for health and well-being.

### Securitization through Everyware

Clearly, one of the main implications of the development of everyware is that it opens up the possibility of widening and sharpening surveillance. Everyware encompasses the threat of universal panopticon (of being monitored at all times in all places), or at the very least, a series of strongly overlapping oligopticons covering many more aspects of everyday activities. Indeed, the preeminent discursive driver in the development of everyware technologies is the rhetoric concerning enhanced safety and security, especially with respect to reducing crime and tackling the threat of terrorism. Everyware promises new opportunities to monitor, link, and make sense of the interactions, transactions, and mobilities of people, goods, and information, at a spatial and temporal resolution previously impossible: to produce a dense, spatialized, rhizomic assemblage of oligopticons that will enable its users to know simultaneously and in the near real time the what, when, and where of everything in the world. Here, a key goal is anticipatory governance (Budd and Adey 2009), wherein three overlapping technologies—those that identify, those that read, and those that interpret—work in unison to create a fine-grained net of automated management (see chapter 5).

If we project this forward, we can imagine a world in which every action is monitored on an ongoing basis and actively shaped by different privileges and entitlements. In the home of this future world, all the activities and every conversation of the occupants would be visible, recordable, and analyzable by software. The household management system would note what time each person went to bed and woke the next morning, and movement patterns between rooms. The system would track the use of appliances; what each person ate, and the intake of any toxins, junk food, or excessive stimulants. The system would note the standard of personal hygiene of each person, the information browsed, television watched, and the e-mail read, written, and sent, as well as discussions on the phone and their content.

Passivity can also be observed in an everyware home; when everything electrical and mechanical (switches, locks, handles) registers a digital event, the periods of human *inactivity* will be as obvious to software as periods of activity. Software might also be able to provide a plausible model of a person's emotional and psychological state from all the observed physical activity and inactivity. This information could be

evaluated automatically to dynamically adjust health insurance payments, carbon taxes, charge for services used, or even discipline for inappropriate behavior.

Similarly, on the daily commute to work, the car and the road system could monitor how the driver is behaving, whether the rules of the road were obeyed, and note the route taken for the purposes of warranty protection, law enforcement, and insurance and toll payments. If the journey is by public transportation, then automatic payment procedures or face-recognition software, or other biometric readers, would record the time and route of the journey for the purposes of billing and public safety. At work, keystrokes, access, and alterations to files, movements within and between buildings, and conversations at meetings and in corridors would all be automatically monitored and used to evaluate work efficiency, productivity, and standards, and to reshape behaviors to those required by the company. In the supermarket, shoppers would automatically be identified, their movement around the store would be tracked, and all the items picked would be monitored regardless of whether they were later purchased; and what is bought would be recorded. This is a world in which spaces of anonymity are negated by everyware and contemporary notions of privacy evaporates; as such, the "disappearance of disappearance" is a genuine possibility (Haggerty and Ericson 2000, 619).

In the world of everyware, intensive surveillance would not be confined to individuals, but also to the manufacture, distribution, use, and disposal of objects. For example, it has been hypothesized that the logical end point of coded objects are spimes (Sterling 2005). A *spime* is a wholly new kind object for which there is an entire recorded history stretching from design and manufacture to disposal/recycling. Such histories will include deep details on: (1) everything used to make, process, and distribute that object, plus protocols for safe and sustainable disposal, (2) everyone and everything that has come into contact with that spime during its lifetime, (3) the context of making and use, including labor relations, cost and profit margin, carbon tax, and patents. In other words, a spime is an object that has a full genealogy wherein the entire actor-network of a thing is knowable and indexical, which, Sterling (2005, 11) asserts, means they are "material instantiations of an immaterial system . . . [they] begin and end as data."

Although no spimes presently exist, there are projects and programs being developed that might be might be termed proto-spimes; that is, they invest objects with spime-like capacity, although their capacities exist external to the thing being recorded. For example, there have been a number of projects to make transparent the full extent of food production (see chapter 9; Buhr 2003; Popper 2007). With respect to agriculture, these are moving beyond existing farm-to-fork tracking systems to much more granular tracing that aims to follow livestock from conception (that is, recording both parents and over time the lineage of all animals and how they were reared) to the consumer's home (through farms, slaughterhouses, logistics chains, and supermar-

kets). In the home of the future, domestic practice would consist of a rhizomic assemblage of spimes and a computationally rich building fabric whose entire history of use and adaptation is known—and known in a very particular and precise way. Sterling (2005) views such spimes as empowering—as providing consumers with information they can use to make informed decisions. Depending on who has access to the information generated, they could also become rich sources of surveillance capta.

### Sousveillance through Everyware

The MyLifeBits system is designed to store and manage a lifetime's worth of *everything*—at least everything that can be digitised.

—Jim Gemmell, Gordon Bell, and Roger Lueder

Sousveillance blends together ideas of personal empowerment and surveillance (Mann et al. 2003). It is the self-monitoring of one's personal life through surveillance technologies, consciously employed and controlled by an individual, with the resulting capta being used to help memorialize and manage one's life. The most common form of sousveillance under development is the notion of a life-log. A life-log is conceived as a form of everyware consisting of a unified, digital record an individual's experiences, captured multimodally through digital sensors and stored permanently as a personal multimedia archive. Activities will be seamlessly and unobtrusively captured by digital technologies that are always on, communicate with each other without human instruction or intervention, and are so pervasive that they cover all aspects of human activity and become so banal as to be unnoticed (CARPE 2004).

The aim of life-log developers is to provide a record of the past that includes every action, every event, every conversation, and every material expression of an individual's life—"the totality of information that flows through a human life" (Johnson 2003, 85)—with the ultimate goal being the simultaneous digitization of *all* cognitive inputs experienced by the brain (all five human senses), such that the life-log would be a digital *parallel* memory of the lived experiences of a person. This log would be augmented with capta not directly experienced, but held unconsciously as biological memories, such as physiological conditions inside the body (blood pressure and heart rate) and external conditions (orientation, temperature, and levels of pollution). All events would be accessible at a future date because a life-log would be a searchable and recallable archive (van Dijck 2005). Such life-logs will constitute new, pervasive sociospatial archives, because inherent in their construction will be a locational record; it will detail everywhere an individual has been.

In contrast to externally produced capta that constitutes surveillance, a life-log generates capta from an interior (or first-person) perspective, where the individual is seen through intimate technologies (that is, technologies that are in service to the individual, such as phones, car, fitness equipment, or wearable computers) with the

capta pooled into a unified, multimedia archive that the person controls. Sousveillance is being complemented by scopophilic (the pleasure in looking and in being looked at) technologies—the conscious self-creation and public sharing of sousveillance, for example, through blogging and Web cams. At present, sousveillance capta is patchy in nature (in terms of what is actually captured), is not continuously collected (rather capta is only generated during use), and individual streams of capta are not being amalgamated into a single, unified life-log. Indeed, the retrieval and reuse of material memorialized is a complex set of practices.

The rationale for life-logging centers on changing the concept of personal computing from a computer for life to "memories for life" (Fitzgibbon and Reiter 2003). In particular, a life-log would: reduce physical clutter (there would be no need for photo albums, CDs, notepads, or books, because all would be stored in the life-log). The life-log would also allow the efficient managing of materialism and enhance domestic and individual productivity (it would be possible to know where every one of a person's possessions were and what conditions they were in). The life-log would enhance productivity and enjoyment of life by allowing the searching for and recalling of events and actions and enhance the management and recalling of frail memories, particularly in an aging population where there might be significant memory loss. The life-log would allow the self-monitoring of health conditions, stress levels, diet and fitness, and other aspects of daily life (systematizing and significantly deepening bodily performance monitoring regimes common across contemporary society; Schuurman 2004).

Significant progress is presently being made within the computer science community in exploring life-logging and the software tools needed to realize its vision. For example, an early project was that of Vemuri (n.d.), a researcher at the MIT Media Lab, who developed a personalized, sound logging system called "What was I thinking," that archives all of an individual's conversations and provides a means to usefully search the verbatim transcripts via visual interfaces. Another prototype, developed at the Microsoft Research Lab was SenseCam, a device which automatically took photographs of the person's environment in response to changing conditions (such as body motion, light levels, and temperature) (Williams and Wood 2004). It was "designed to act like a black box for the human body" (Twist 2004), with a custom-built digital camera worn like a necklace, with an ultra wide-angle lens that captured a 132 degree view in front of the wearer. The results of *SenseCam* was a timeline of hundreds of photographs that log activities and spaces as they are encountered throughout the day, which can be interrogated alongside the sensor logs.

Life-logs pose significant implications to the recording of the present, and thus how the past is recalled as opposed to how it is remembered (Allen 2008; Dodge and Kitchin 2007b). Like surveillance more generally, sousveillance also raises a number of social and ethical questions concerning who would own life-logged capta, how it could be

used, and the limits to what is captured. In relation to ownership, while the capta within a life-log would be autobiographical, and would be held by the individual, there are questions concerning access and control. For example, who would have the right to access the life-log, other than the creator? To what extent could the material be sequestered for legal cases, and what would the legal status of such material be? Would capta take on the same status as biological memories? Or would they be seen as *more* objective and true? What would happen when a discrepancy arises between the statements of individuals and the life-log's capta? Would any third parties be able to have access, such as government security agencies or employers? Would access by third parties (including legal use) be restrictive or nonrestrictive (for example, would all capta be available, or only selected portions either by date or by recording medium)? Would other people captured by the life-log have a claim to access its contents (such as a partner, friends, or work colleagues)? What would happen to the life-log at death? What would the inheritance rights be? Who would have control of a child's life-log? Would life-logs be voluntary, or could pressure or mandatory measures by the state force people to adopt them?

The vision of life-logs is that they capture all possible capta, storing it forever. It is not clear, however, to what extent a life-log could be editable, if at all. Should a life-log be modifiable like a diary entry or should it be a photographic image? Should portions be open to selective, permanent erasing? Or just deletion from view, but with the prospect of recovery? Further, should these acts of erasing or deleting themselves be witnessed and remembered by the life-log? Are there events and actions that should be excluded from capture or should there at least be an option to suspend recording? Should you be able to press pause on the life-log? Would an act of deletion or suspension itself be considered a sign of guilt, if the life-log were to be used in a court of law? Do all the mundanities of life really need to be captured for all eternity, such as cleaning the house, walking the dog, or daydreaming in the office? As Oscar Wilde (1988, 80) stated, "One should absorb the color of life, but one should never remember its details. Details are always vulgar." In addition, to what extent would it be possible to dupe the log, to unsettle the authenticity of the record? There is also a case to made for the personal and communal benefits of forgetting events. Accordingly, Allen (2008, 57) warns that "not only might an individual's own life-log problematically preserve a record of bad luck and mistakes, the life-logs of others with whom the individual has come into contact might do the same. Yet people typically have a legitimate moral interest in distancing themselves from commonplace misfortunes and errors. In order to create that distance, they need to be safe from memory: they need to forget and need others to forget, too."

The degradation of biological memory through normal aging or through cognitive disorders are traumatic experiences, as the evidence from forms of dementia and mental illness illustrate. Taking this into consideration, what would be the impact of

accidental or deliberate damage to, or alteration through the planting of false "memories" into the life-log? Moreover, could the life-log be stolen and used, perhaps in the same way as stolen passports or identity cards? What would be the consequences for the person whose life-log was stolen—both emotionally and materially?

Some questions about the real-life aspects of trying to live in a life-logged world are starting to be thought through and questioned, for example in the work of digital artists. One of these, Lucy Kimbell, through her web site (www.lucykimbell.com), "I measure therefore I am" has undertaken an exhaustive quantitative personal audit—which includes her stock market style evaluation called *LIX*, "a weekly index that tracked [her] performance between 2002 and 03 by measuring financial, emotional, social, and environmental factors." Multimedia artist Ellie Harrison's projects include *Gold Card Adventures*, a self-logging of all her public transport journeys for a year, and the *Eat 22* project where everything she ate for the year after her twenty-second birthday was self-photographed, logged, and displayed online (www.ellieharrison.com). Another work is Alberto Frigo's visual-statistics project that questions human beings' banal dependence on technology through a very exacting type of logging. The project is "an ongoing experiment consisting of photographing each time my right hand uses an object in order to create my autobiography for self-reflection and enforcing my identity" (Frigo 2004, 52).

## The Dangers of Everyware

> You had to live—did live, from habit that became instinct—in the assumption that every sound you made was overheard, and except in darkness, every movement scrutinised.
>
> —George Orwell

As we have detailed above, and in chapter 5, the use of software in everyday life is changing the how governance unfolds. New forms of regulatory technologies are qualitatively and quantitatively transforming the nature of surveillance, both deepening the level of discipline, and actively reshaping individual behaviors. Given the potential of everyware to widen and deepen the oligoptical nature of surveillance, it seems pertinent to question whether the work of code across daily practices is inevitably leading to an automated form of Big Brother? Taken from Orwell's novel *Nineteen Eighty-Four*, Big Brother is the name of a system of totalitarian social control where people live within an almost perfect panopticon that renders them amenable to constant surveillance and self-discipline from fear of betrayal, and accordingly differential access to work and consumption.

It is certainly the case that the automated management produced within an everyware future has the potential for creating something like a Big Brother scenario. As examined in chapter 5, the rollout of surveillance technologies, based upon captabases

and software algorithms, in recent years has significantly increased the generation of capta about whole populations and extended individual capta shadows through time and across everyday domains of living. While a capta shadow is inevitable and necessary to be able to function in contemporary society (for example, to work legitimately and pay taxes, to access government services, to have a bank account and borrow money, to legally own and drive a car, to travel internationally, to receive medical treatment, or to buy most commodities, Clarke 1994b; Lyon 2002), the amount and type of capta generated extends well beyond that needed to assess responsible citizenship and facilitate democratic participation. Further, becoming a subject of surveillance systems can be inadvertent, unknown, or against a person's wishes (Greenfield 2006).

This would be extended further in a world populated by everyware, and is likely to occur through technologies that were not initially envisioned as fulfilling such a role. Again, this process of "control creep" (Innes 2001), wherein capta generated for one purpose is kept and reused for another is already in evidence in today's society. Control creep can perhaps be best seen in action with regard to the intensification of security screening and surveillance, including the rise of intensive profiling and biometric authentication, whereby capta generated for one purpose is then used to profile passengers, or capta held by one agency is then shared with another that previously had no rights to access it (Lyon 2003). In the former case, existing administrative identification and record-keeping infrastructures are being remodeled as part of generalized anti-terror surveillance and risk-reduction apparatus. For example, the London Congestion Charge system was sold to the public on the basis that the capta on license plates, generated automatically from a grid of cameras, would only be used for administering congestion charge payments between 7 a.m. and 7 p.m. during weekdays. However, it is now used twenty-four hours a day and is also available as an effective surveillance system for all forms of crime under the rubric of tackling security issues (Ford 2007).

There are genuine reasons to be concerned about control creep and pervasive surveillance, especially when accompanied by legislation that gives states and companies ever more rights to monitor people unencumbered by independent oversight and effective rights of redress. As Andrejevic (2007) notes, legislation post-9/11 in the United States, for example, the USA PATRIOT Act (2001), gave the government extended powers to observe U.S. citizens while at the same time making the nature of that monitoring exempt from the Freedom of Information Act. At present, there are still opportunities to hide in the crowd, but if workable face recognition software could be developed to scan whole streets and identify its occupants, and cross-reference that to itineraries of where people should be, then the specter of Big Brother would take a significant step nearer to reality.

If life-logs are added to this mix and are made accessible to third parties, then the nature of an individual's capta shadow becomes all-encompassing, opening the way

for highly invasive profiling, social sorting, and pernicious disciplining effects. Life-log capta could extend social sorting practices, allowing for preferential treatment of customers and clients that maximizes profits and maintains the status quo, and penalizes those that fit certain profiles (Gandy 1993; Graham 2005; Lyon 2003). Moreover, there is the potential for personal indiscretions, idiosyncratic interests, and minor infractions of the law to be identified and criminalized, thus encouraging more rigorous, self-disciplining behavior, and the development of an ultra-conservative society (Blanchette and Johnson 2002). When every action is recorded for perpetuity, in a seemingly objective manner, and it is likely that the consequences will be realized, then a panopticon starts to become possibility. To address these issues, Greenfield (2006, 235) suggests that everyware must:

- Default to a mode that ensures physical, psychic, and financial safety
- Be self-disclosing (people should know they are in the presence of everyware)
- Be conservative of face (people should not lose dignity due to everyware)
- Be conservative of time (everyware should not introduce undue complications into everyday operations)
- Be deniable (people must have the ability to opt out, always and at any point of systems they own)

We have previously contended that systems of pervasive computing should be engineered from the beginning to include elements of forgetting (Dodge and Kitchin 2007b; see chapter 11). We argued that "forgetting is not a weakness or a fallibility, but is an emancipatory process that will free life-logging from burdensome and pernicious disciplinary effects" (p. 441). While Greenfield's six point plan and our own "ethics of forgetting," are both laudable notions, the extent to which they will be built into future systems is doubtful, given the history of surveillance and how states treat their citizens and corporations their customers.

Beyond the dangers of pervasive surveillance, everyware creates a situation of over-reliance on a range of interlinked and interdependent technologies. A catastrophic failure of everyware could lead to widespread economic and social paralysis as multiple systems fail in a cascade without manual alternatives (the RISKS list posts a growing range of examples of the unforeseen problems and sometime subtle failures of current software systems, http://catless.ncl.ac.uk/Risks). At a more localized scale, any object that is networked is open to hacking and reconfiguration, potentially creating havoc with home and personal appliances (Mitchell 2004). In addition, there are dangers concerning identity theft whereby tokens of identity can be used to access financial and other records, potentially causing serious harm to the finances and status of the victim; harm that is presently difficult to repair. Collateral damage is also caused by errors in capta generation so that innocent victims end up on no-fly lists, or are barred entry to countries, or are denied access to services. Such errors are presently not

uncommon. For example, as detailed in chapter 7, air travel captabases are known to have substantial biographical errors (typos, nonupdates, and missing or misleading fields) and biometric errors.

The rollout of everyware risks overcomplicating aspects of daily life that at present are relatively straightforward. For example, a typical home still largely consists of a set of relatively autonomous technologies that perform specific domestic tasks. In a smart home, where these technologies become interlinked and work in conjunction with one another a new layer of backgrounded complexity would be introduced in the running of the household in order to provide certain efficiencies and benefits. In this case, if the home management system were to fail, many domestic practices could not proceed as intended. We presently experience such moments during rare power outages that highlight how dependent many domestic practices are on the availability of electricity.

For McCullough (2004) one of the dangers of everyware is the potential for introducing new levels of frustration and inconvenience into basic operations of people's lives—a proliferation of autonomous annoyances (things constantly trying to interfere in and mediate daily lives). The reason why there was a successful transition from manual and mechanical labor to electrically powered work was that there were significant gains in effort expended, time, scale, and convenience. For example, the washing machine gave significant benefits over washing clothes by hand, and the electric oven gave benefits to cooking compared to an open fire. Going the next step, and adding computational power to the washing machine and oven would need to deliver additional benefits without making their use more cumbersome or inconvenient. An appliance that comes with a hefty "how to" booklet for a machine that replaces a relatively simple task suggests excessive functionality. A straightforward dial or a couple of selection switches are not improved by being replaced by an overwhelming choice of menus, options, and check boxes on a screen. It is likely in such scenarios that many people will simply fall back on default settings that seem to work, a point echoed with earlier rounds of complex electronic home technology, such as the VCR where large numbers of people failed to program them successfully, and simply used them as basic playback devices (Rode, Toye, and Blackwell 2004).

Given the wholesale transfer to digital information storage, including people's own personal records such as financial statements or photographs with sentimental value, risks also exist with respect to file safety and security. Relying on software to keep digital media safe is often compounded because most people are poor at maintaining systematic backups, or any backup at all, and where these records are stored on a networked device they become potentially vulnerable to unauthorized remote access and theft.

Other than consumer resistance along political or ethical lines, a critical problem that everyware has to overcome in order to become truly embedded as an everyday

background to ordinary life, is to be flexible enough to be contextually adaptable to the messy, contingent, and fluid circumstances through which people's daily lives unfold. To be able to deal with the moment-to-moment ways that problems are encountered and solved is much more complex than the representational models and evaluative algorithms in present day software systems. For McCullough (2004) everyware needs to be context sensitive for it to be useful and successful. Perhaps somewhat paradoxically, everyware cannot operate in a universal fashion, as if all places and people are the same, but rather needs situational protocols able to handle subtleties of local circumstances. For Dourish (2001), this means everyware has to be a form of social computing—software systems that are designed with human context in mind. Developing such social computing represents an enormous technical challenge.

## The Partiality of Everyware

> The networks of control that snake their way through cities are necessarily oligoptic, not panoptic: they do not fit together. They will produce various spaces and times, but they cannot fill out the whole space of the city—in part because they cannot reach everywhere, in part because they therefore cannot know all spaces and times, and in part because many new spaces and times remain to be invented.
>
> —Ash Amin and Nigel Thrift

Given some of the potential dangers of everyware, it is perhaps fortunate that the software technologies of everyware, for the foreseeable future, will be unable to produce a panopticon—there will always be gaps and blind spots for a variety of reasons. As such, systems of software-enabled surveillance remain, and will continue to remain, oligoptical in nature. Although they will be more efficient and powerful, they will still be open to vertical and horizontal fragmentation.

For everyware to work effectively and efficiently as coded assemblages, technologies must be able to internetwork and the capta held within systems must have a high degree of interoperability. As Greenfield (2006) notes, however, even environments that are highly saturated with software-enabled technology largely operate as a constellation of separate systems as there are few established protocols to enable internetworking. For example, in chapter 8, very few of the codejects we detailed can presently communicate and interact with each other automatically; they simply interface with the home's occupants, who can transcribe and translate settings and information as necessary. And yet, the various devices embedded within an environment need to be able to talk to each other if the system is to become more than the sum of its codeject parts (McCullough 2004). Even if they did work in harmony, Greenfield (2006) notes that any assemblage would be so densely woven and complex that in the event of a breakdown it might not be possible to diagnose where the fault lies. As new software

is rolled out over time, new problems emerge concerning how to effectively interface these with a diversity of legacy systems. Critical to the success of everyware, then, is the ability of each system in the assemblage to self-recalibrate when new devices are added (McCullough 2004). This is no easy task, especially as altering legacy systems is difficult given that its code is old, has been worked on by many programmers over time, and it is unlikely that any one person understands it well enough to make significant changes (Ullman 1997). The difficulties of keeping a contemporary PC running efficiently and securely as it tackles all manner of tasks is a taste of the coming challenges of making everyware a reality.

If we consider the issue of interoperability, there are large variations in the form, units, and standards of capta generated by different software systems that severely limit the ability to use records from one system in another, or to marry details from two different captabases. This is compounded by the fact that most captabases have some degree of error caused by mistakes at the capture stage. Addressing the issue of capta interoperability is not a trivial exercise given the vast proliferation of agencies and companies around the globe producing new software products that generate voluminous quantities of capta, often creating new formats and standards (see figure 10.5). (This is often due in part to the economic strategy of product development that seeks to lock in customers.) Even if these organizations worked closely with each other to ensure compatibility with regard to things such as capta formats and ontologies (often difficult because they are commonly in competition with each other); and if further international capta standards and conventions were put in place; even if national and transnational capta infrastructures that provide common frameworks and standards across borders and platforms were created; and if detailed metacaptabases (capta about capta) that document how proper records are created by different agencies and their attributes were produced, there would still be significant gaps in capta coverage and interoperability that would limit surveillance to be oligoptic in nature, rather than panoptic.

The partiality of present forms of surveillence can be seen with respect to the governance of driver behavior, vehicles, and roads, which is uneven in nature and experienced unequally. At a basic level, there is a marked variation in the extent to which automated technologies are deployed within driving infrastructures. At the macroscale, there are large variations among cities and countries, depending on government policy, institutional will, and spending regimes. For example, Britain has embraced to a much greater degree the rolling out of such infrastructure than, say, Ireland. And within Britain, London has had a disproportionate investment in such systems compared to other cities. In part, this is because of the severe congestion in the city and its strategic economic importance to the nation, but also because of wider antiterrorist initiatives. At a more local scale, major highways are much more likely

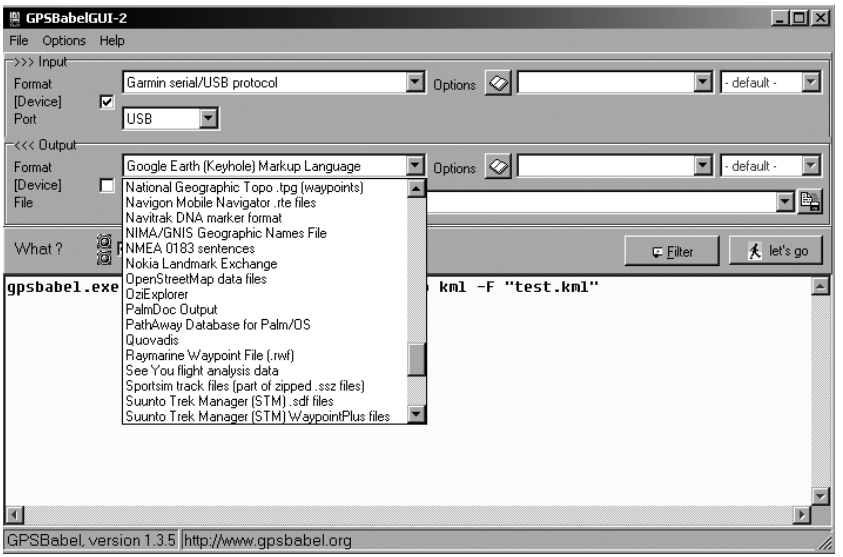



**Figure 10.5**
A prosaic example of the pragmatic constraints on everyware being built to handle the numerous formats for spatial capta, such as generated by GPS. Here, a purpose-built software tool called GPSBabel converts between many of the common formats.

to be surveyed and regulated through automated software systems than minor roads and residential streets. (These unwired places in the assemblage have often been subject to alternate, physical traffic calming, such as the disciplining of drivers through "dumb" features as road humps, chicanes, and width constrictions.) This is because the volume of traffic needs to be regulated with regard to flow and tolls. In addition, there is an uneven application across drivers and vehicles. For example, depending on age and previous penalties, drivers can be sorted by software with regard to insurance, or financing for buying vehicles. Newer and more expensive vehicles are more likely to be full of various coded systems relating to sophisticated engine management systems and GPS navigation tools (see Dodge and Kitchin 2007a). This partiality will continue for some time, if for no other reason than the cost to retrofit, monitor, and regulate the entire system, and the legacy effects of old vehicles and infrastructure.

We now look at the smart home example. The extent to which smart homes, as envisioned by some technologists, will come to fruition is doubtful. While it is evident that code is increasingly becoming part of everyday domestic life and does make a difference to how domestic practices unfold, any transition to the era of the smart

home will take place over a long period of time (see chapter 8). With respect to the adoption of coded objects, many household tasks continue to be solved by analog appliances and tools that will, in many cases, be used until they need to be replaced. In other circumstances, coded objects are expensive luxury items that require a certain income, lifestyle, and technical literacy to purchase and operate (Rode 2006). Whole swaths of contemporary societies, including large segments in the West, live at or below the poverty line and only have sufficient income to meet essential bills for housing, fuel, and food. For these people, with little or no disposable income, many of the smart technologies being developed are not accessible or even desirable (though many personal gadgets such as iPods and cell phones are).

With respect to the development of computationally rich building materials, this will require extensive and expensive retrofitting of existing dwellings that is unlikely to be untaken without significant benefits to the household or else by force of external regulatory pressure (such as being a requirement of mortgage lenders/insurers or waste/energy reduction in the name of more sustainable living). At present, it is unlikely that such adaptations will offer such tempting benefits especially with the rapid redundancy that currently accompanies technological change. In other cases, people simply do not see the utility of living in homes that respond to them in new ways—they do not need or desire a home management system, they are content with their domesticity as it presently unfolds. Indeed, everyware sometimes seems like a technology that is being driven by what is technically feasible and the marketing engine of companies, rather than by a genuine demand among consumers. (To put this into perspective, the initial domestication of electricity also had to be heavily marketed as people did not see it as essential to daily life.) What this means is, as with the adoption of any set of technological innovations, the adoption of everyware will be uneven and unequal, both socially and geographically, depending on the person, the place, and changing circumstances.

## Resisting Everyware

Everyware will also remain partial because its pernicious surveillance will be questioned and resisted by some people. Surveillance and automated management is contingent, relational, and negotiated in nature, and unfolds in multiple ways, shaped by how people interact with and resist the systems employed to survey and manage them. As Lyon (2007) notes, some people deliberately hide their faces from security cameras, falsify information, consciously switch devices off, and otherwise dissimulate, and negotiate with those that survey them. Surveillance is not a "static, relentless or unyielding process. . . . It is malleable, flexible, and the product of game-like processes . . . where the outcomes are far from determined in advance" (Lyon 2007, 165). Forms of resistance range from avoidance, partial compliance, subversion,

and campaigning for wholesale change. Indeed, Marx (2003) details eleven different ways that surveillance is resisted by individuals (elements of which often work in unison).

*Discovery* A person finding out if they are under surveillance (using some kind of detecting device).
*Avoidance* The evasion of surveillance (taking a route that has no cameras) or not purchasing software-enabled versions of analog technologies.
*Piggybacking* Using another person or object to avoid surveillance (following someone with a security pass through a secure door).
*Switching* Using the identity of another person (using someone else's security pass to gain admittance through a secure door).
*Distorting* Manipulating the results of surveillance so that they are misinterpreted (holding down a key so that it appears that a large number of keystrokes have been performed).
*Blocking* Hiding a feature that might identify a person (wearing a hat or hooded sweatshirt that obscures the face).
*Masking* Using a false identity (using a false name to access a web site).
*Breaking/hacking* Vandalizing surveillance technology so it no longer works (placing something across the lens of a camera or attacking its supporting software with a virus).
*Refusing* Refusing to impart a piece of information (refusing to fill out certain fields on an application).
*Cooperation* A third party prevents or erases surveillance (a confederate removes the evidence of surveillance from the record).
*Countersurveillance* Surveilling the surveillers in an effort to get them to limit their activities (making it widely known that a company is using surveillance to discriminate against customers; the aim of the counter-surveillance tactic would be to incite customers to move their business elsewhere).

Clearly these resistance techniques to surveillance depend, in part, on knowing when and where to deploy them. This is possible to some degree with partial and visible surveillance technologies, but much more problematic when software is used in capture systems where the practice is itself the means through which one is monitored (see chapter 5).

If we examine systems which have heavily deployed software-enabled surveillance, all of these forms of resistance can be evidenced. For example, if we again consider the governance of driving and roads in the UK, an infrastructure that is heavily monitored and regulated through road taxes, licensing, insurance, and traffic management systems, we can see wholesale resistance and subversion in actions such as driving above the speed limit in unmonitored areas, avoiding routes that are actively moni-

tored, driving a stolen vehicle, driving without paying tax and insurance, using false plates, using GPS enabled technologies to give advance warning of detection devices, vandalizing speed cameras, claiming that the vehicle was being driven by someone else, hacking car code to alter a vehicle's performance, and using homemade, illegal "traffic signal pre-emption devices" to alter traffic light sequences, and the vandalizing of cameras (Dodge and Kitchin 2007a). The extent to which the system is partial in its actions and effectiveness varies between activities, but as an illustration, estimates put the extent of uninsured driving in the UK at one vehicle in twenty (DfT 2004). These individual actions are being complemented by wider protests against some technologies, such as the vocal campaigns against speed cameras in the UK, which have argued that employment of automated management is more about local revenue raising than improving road safety.

## Conclusion

In this chapter, we have considered how the current state of play with regard to the embedding of software into everyday life, might evolve into everyware—that is, the calculative capacity of code being distributed and available at any point on the planet. Everyware seeks to transform people's experience by producing interactions with software that "feel natural, spontaneous, human" (Greenfield 2006, 1). It is clear that the development of everyware will consist of the interweaving of a number of related forms of software—pervasive, ubiquitous, sentient, tangible, wearable computing—that all seek to transform how we interact and live with code. A core objective is to produce calm technology—software that people are comfortable using because it is so easy to interface with that it becomes a normal, unconscious practice. In so doing, it fades into the background, becoming part of the everyday experience. We have illustrated what such a future might look like by examining, in brief, everyware in relation to the discourses and materialities of empowerment, securitization, and sousveillance.

In the second part of the chapter, we examined some of the dangers and social risks associated with a state of everyware, and the extent to which everyware as envisioned by some commentators might come to fruition. Pervasive surveillance and sousveillance has the potential to produce a society that never forgets—that has a permanent sociospatial archive of trillions of events across a whole population, traceable through space and time; a detailed spatialization of the history of everything, everywhere. Paradoxically, everyware could well complicate life and introduce new technological hazards at the same time it seeks to make life simple and reduce risk. Some aspects of everyware are likely to become a standard part of everyday life, especially in cities, such as wireless access to networks. Cell phone coverage is already widespread in many countries, providing increasing seamless access to

software systems regardless of location. The embedding of code into infrastructure and the rollout of smart management systems is likely to be much more uneven and unequal in access. The extent to which different software systems and captabases, produced for dissimilar reasons at different times, can become highly interoperable and adaptive to new additions is questionable. Further, aspects of everyware will be resisted in a variety of ways by individuals and communities. As a result, everyware, while striving to be universal in nature, will inevitably be partial.

This is a section of doi:10.7551/mitpress/9780262042482.001.0001

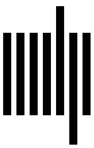
# Code/Space

## Software and Everyday Life

By: Rob Kitchin, Martin Dodge

## Citation:

*Code/Space:* Software and Everyday Life
**By:** Rob Kitchin, Martin Dodge
**DOI:** 10.7551/mitpress/9780262042482.001.0001
**ISBN (electronic):** 9780262295239
**Publisher:** The MIT Press
**Published:** 2014



The MIT Press

This book was set in Stone Sans and Stone Serif by Toppan Best-set Premedia Limited. Printed and bound in the United States of America.

Library of Congress Cataloging-in-Publication Data

Kitchin, Rob.
Code/space : software and everyday life / Rob Kitchin and Martin Dodge.
p. cm. — (Software studies)
Includes bibliographical references and index.
ISBN 978-0-262-04248-2 (hardcover : alk. paper)
1. Computers and civilization. 2. Computer software—Social aspects. I. Dodge, Martin, 1971– II. Title.
QA76.9.C66K48 2011
303.48′34—dc22

2010031954

10 9 8 7 6 5 4 3 2 1