Some guidelines for the ethical development of ubiquitous computing

By Adam Greenfield*

Studies and Observations, 343 East 30th Street, New York, NY 10016, USA

At a time when both the landscape of everyday life and the choices available to us there are increasingly conditioned by ubiquitous information processing systems, it seems wise to articulate some general principles guiding their ethical design and deployment. I here enunciate five broad guidelines for the designers of such systems, including recommendations that they be devised in such a way as to default to harmlessness, be conservative of time, be conservative of face, be self-disclosing and be deniable. I conclude with some observations about the likelihood of any such principles winning usefully widespread voluntary adherence.

Keywords: ubiquitous computing; ethics; everyday life

1. Introduction

Over the last several years, a very wide variety of technical systems with the capacity to sense, process, transmit, represent and take physical action on digitally encoded information have been deployed in the everyday life of the developed global North. Whether or not such systems hew to classically Weiserian (Weiser & Seely Brown 1996) notions in either their provisions or their effects, it is now possible to assert that ubiquitous computing is a de facto daily reality for hundreds of millions of users. As a result, that which conditions choice and action in the everyday environment is already no longer primarily physical, but resides in large part in the invisible and intangible overlay of digital information that enfolds it.

Since the broad outlines of this novel paradigm first became clear, around the turn of the millennium, careful consideration has been given to the complications of user interactions with systems situated in everyday space and time, and especially how such interactions depart from the familiar conventions of the desktop (Dourish 2001; Bellotti et al. 2002). Given all of the ambitions subsumed under the rubric of ubiquitous computing, however, there has been relatively little discussion of specifically how such systems might protect the prerogatives of their users. From the perspective of a non-academic considering the profound implications of ubiquitous computing for privacy and civil liberties,

*ag@studies-observations.com

One contribution of 19 to a Discussion Meeting Issue ‘From computers to ubiquitous computing, by 2020’.
social interaction and the presentation of the self, and the presumptive desire of most users to lead lives free of complication and hassle, this seems worrisome (Greenfield 2006).

What may be still more worrisome is that, as Bellotti & Sellen (1993) emphasize, not every party developing and deploying ubiquitous systems will always esteem the abstract needs of users more highly than market share, the profit motive or the prerogatives of total information awareness. Even where developers can be relied upon to act in good faith, they will require practically useful guidance.

Much of the discourse around ubiquitous computing, and a similar proportion of the available literature in the field, has to date been academic and descriptive in nature. But, however useful such descriptions are, they are not particularly well suited to discussions of what ought (or ought not) to be built. By contrast, the designer working under the pressures and constraints of contemporary technological development practice will need relatively clear-cut principles to abide by, and to wield in discussions with colleagues and superiors.

Accordingly, I aim here to develop a strategy for ethical development that does take this need into account; that spells out the relevant issues in sufficient detail to be of use to developers; that strikes a balance between their needs and those of users; and that incentivizes compliance rather than seeking to punish non-compliance.

I here articulate five principles for the ethical development of ubiquitous systems, even as I acknowledge that any such set of principles is bound to be contingent, provisional and incomplete at best.

2. Five principles for the ethical development of ubiquitous computing

(a) Ubiquitous systems must default to harmlessness

The first of our principles concerns what happens when ubiquitous systems fail. ‘Graceful degradation’ is a term used in engineering to express the ideal that if a system fails, if at all possible it should fail gently in preference to catastrophically; functionality should be lost progressively, not all at once. A Web browser might be unable to apply the proper style sheet to a site’s text, but it will still serve the unstyled text instead of leaving the user gazing onto a blank screen; if a car’s antilock brake systems module fails, the driver loses the augmentation it offered, but is still able to manually press down on the brake pedal in order to slow the car.

This is sound engineering practice. I believe, however, that given the expanded assumption of responsibility for the human user inherent in ubiquitous systems, graceful degradation does not go far enough.

Ubiquitous systems must default to a mode that ensures users’ physical, psychic and financial safety. Note that this is not an injunction to keep users safe at all times, an aim as unattainable as it would be undesirable. It is simply, rather, a strong suggestion that when ubiquitous systems break down—as they surely will from time to time, just like every other technical system that humanity has ever imagined—they should do so in such a way as to safeguard the people relying on them.
What precisely ‘safety’ means will obviously vary with place and time. Even as regards physical safety alone, for example, in the USA, we currently find ourselves in a highly risk-averse era, in which public fear and litigiousness place real limits on what can be proposed. Meanwhile, coming to agreement as to what constitutes psychic and financial safety is probably more culture-dependent still. It is entirely possible that working out a definition of safety restrained enough to be shared broadly will leave few parties wholly content.

Nevertheless, given that the systems under contemplation engage the most sensitive things in our lives—bodies, bank accounts and very identities—we should demand that a commensurately high level of protection be afforded them.

(b) Ubiquitous systems must be self-disclosing

The second principle concerns provisions to notify us when we are in the presence of some informatic system, however intangible or imperceptible it otherwise may be.

The systems under discussion here are hard to see for a variety of reasons, some circumstantial and some intentional. Information processing can be embedded in mundane objects, secreted away in architectural surfaces, even diffused into behaviour. And as much as this may serve classically ‘encalming’ ends (Weiser & Seely Brown 1996), it also lends itself to too many scenarios in which personal information, including that of the most intimate sort, can be collected without the user’s awareness, let alone his or her consent.

Given the degree, further, to which ubiquitous systems are almost by definition networked and globally interconnected, such information can easily, even inadvertently, be conveyed to parties unknown to the user. Such data persist on the network in a kind of uncanny afterlife, there to be retrieved in contexts arbitrarily remote in space and time from their origin (Marx in preparation). Simply put, therefore, users should be told: what kinds of information-gathering activities are transpiring in a given place; what specific types of information are being collected; by whom and for what purpose; and, finally, how and in what ways the information-gathering system at hand is connected to others.

We might express such an imperative like this: ubiquitous systems must contain provisions for immediate and transparent querying of their ownership, use and capabilities.

Whether such disclosures are made verbally, graphically or otherwise, they ensure that the user is empowered to make informed decisions as to the level of exposure he or she wishes to entertain.

So, for example, if the flooring in eldercare housing is designed to register impacts, it should say so, as well as specifying the threshold of force necessary to trigger an alert. It should enunciate what precisely is supposed to happen if the flooring does register a fall, and, if the flooring is connected in some way to a local hospital or ambulance dispatcher, just which one.

None of this is to say that users should be confronted with a mire of useless detail. But ‘seamlessness’ must be an optional mode of presentation, not a mandatory or inescapable one. Less ominously, such seamful disclosure will also serve to inform us when otherwise intangible services are available.
When an otherwise unremarkable object affords some surprising functionality, or when a digital overlay of information about some place exists, we need to have some way of knowing these things that does not itself rely on digital mediation; Arnall (2005) has developed a vocabulary of graphic icons that communicate ideas like these, a friendly, human-readable equivalent of the ‘service discovery layer’ in Bluetooth that specifies what devices and services are locally available. Whether we use them to protect ourselves from intrusive information collection, or to discover all of the ways in which our new technology can be used, such provisions for transparent self-disclosure will be of critical importance in helping us find ways to live around and with them. Such knowledge is the basis of any meaningful ability on our part to decide when and to what degree we wish to engage with these systems, and when we would prefer not to.

(c) Ubiquitous systems must be conservative of face

Something too rarely considered by the designers of ubiquitous systems is how easily their ordinary operation can place a user’s reputation and sense of dignity and self-worth at risk.

The science fiction writer Disch (1973) illustrates this scenario beautifully in his novel 334; in particular, 334’s casual sketch of what would later be known as an Active Badge system. Disch shows us not the convenience or logistical efficiency of such a system, but how it might humiliate its human clients, in this case the ageing, preoccupied hospital attendant Arnold Chapel. Embroiled in an illicit plot, Chapel has distractedly allowed himself to wander from his course, and is audibly corrected by the hospital’s pervasive traffic control system:

“Arnold Chapel,” a voice over the PA said. “Please return along ‘K’ corridor to ‘K’ elevator bank. Arnold Chapel, please return along ‘K’ corridor to ‘K’ elevator bank.”

Obediently he reversed the cart and returned to ‘K’ elevator bank. His identification badge had cued the traffic control system. It had been years since the computer had had to correct him out loud.

All that was, in fact, necessary or desirable in this scenario was that the system return Chapel to his proper route. Is there any justification, therefore, for the broadcast of information embarrassing to him? Need the correction be perceptible to anyone but Chapel himself? Why humiliate, when adjustment is all that is mandated?

Of course, no system in the world can keep people from making fools of themselves if they are bound and determined to do so. About all that we can properly ask for is that our technology be designed in such a way that it is *conservative of face*: that ubiquitous systems must not act in such a manner as would unduly embarrass or humiliate users, or expose them to ridicule or social opprobrium, in the course of normal operations.

I argue, therefore, that some degree of plausible deniability, including above all imprecision of location, is highly useful, such that even (natural or machine assisted) inferences about intention and conduct may be forestalled at will.

Chalmers et al. (2003) described an ultrasonic location system as ‘subject to error, leading to uncertainty about … position’, and, as they recognized, this imprecision can within reasonable limits be a good thing. It can serve our ends,
by giving anyone looking for an individual most of the information they need about where that person is, but not a pinpoint granular location that might lend itself to unwelcome inference; the block scale, in other words, or even that of the neighbourhood, but not the metre scale.

The degree to which location becomes problematic depends to some extent on which of two alternate strategies is adopted in presenting it. In a ‘pessimistic’ presentation, only verifiably and redundantly known information is displayed, while an ‘optimistic’ display includes possibles, values with a weaker claim on truth. The less parsimonious optimistic strategy obviously presents the spectre of false positives, but if this is less than desirable in ordinary circumstances, in this context, a cloud of possible locations bracketing the true one might be just the thing we want. Still worse than the prospect of being nakedly accountable to an unseen, omnipresent network is being nakedly accountable to each other, at all times and places.

There are, at least occasionally, legitimate social purposes for shame. But we are not talking about doing away with shame. The issue at hand is preventing ubiquitous systems from presenting our actions to one another in too perfect a fidelity, in too high a resolution, and therefore keeping us from maintaining the beneficial illusions that allow us to live as a community. We must build ourselves safe harbours in which to shelter from an accountability that otherwise tends towards the total.

Finally, there is the humiliation and damage to self-worth we experience when we simply cannot figure out how to use a poorly designed technical system of any sort. Sadly, no principle or guideline, however strongly stated, however widely observed, can ever endow all the world’s designers with equal measures of skill, diligence and compassion; nor could any guideline ensure that designers are afforded the time and space they require to work out the details of humane systems. What we can insist on, however, is that those tasked with the development of ubiquitous systems be reminded of the degree to which our sense of ourselves rides on the choices they make.

(d) Ubiquitous systems must be conservative of time

One of the reasons that Fukasawa’s (1999) vision of information processing dissolving in behaviour is so alluring is because it promises to restore simplicity to our daily activities. As Mainwaring et al. (2005) emphasize, daily life in the developed world now exposes us to a multitude of physical and informational infrastructures, each of which requires some kind of token to mediate. Simply to get through the day, we carry keys, cash, credit cards, debit cards, transit passes, parking receipts, library cards, loyalty programme cards and so on, and the list is anything but comprehensive.

In the course of a single day, moreover, we may use any or all of an extensive inventory of digital tools and devices, each of which has a different user interface, each of which behaves differently: music and video players; telephones; personal computers; cameras; cable and satellite television controllers; automated teller machines (ATMs); household appliances; and even vehicles.

Ubiquitous systems promise to replace this unseemly shambles with a rather more compact and intuitive complement of interface provisions, requiring far less of our time, energy and attention to deal with. The appeal of this paradoxical
vision—high complexity, in the service of the simple—should not be underestimated. But the inevitable flipside of it, at least if our experience with other information technologies is an accurate guide, is that almost all users will face the prospect of wasted time and effort at one time or another.

Philip K. Dick, never one to overlook the all-too-human complications inherent in any encounter with high technology, depicted more than one hapless protagonist wrestling with ornery or outright recalcitrant pervasive devices. In his 1969 novel *Ubik*, Joe Chip gets threatened with a lawsuit by his front door:

The door refused to open. It said, “Five cents, please.”

He searched his pockets. No more coins; nothing. “I’ll pay you tomorrow,” he told the door. Again he tried the knob. Again it remained locked tight. “What I pay you,” he informed it, “is in the nature of a gratuity; I don’t have to pay you.”

“I think otherwise,” the door said. “Look in the purchase contract you signed when you bought this [apartment].”

In his desk drawer he found the contract...Sure enough; payment to his door for opening and shutting constituted a mandatory fee. Not a tip.

“You discover I’m right,” the door said. It sounded smug.

From the drawer beside the sink Joe Chip got a stainless steel knife; with it he began systematically to unscrew the bolt assembly of his [apartment’s] money-gulping door.

“I’ll sue you,” the door said as the first screw fell out.

Joe Chip said, “I’ve never been sued by a door before. But I guess I can live through it.”

And this is just to get out of the house and on with the day. Self-important doors are probably not even the worst of it, either; this is the kind of moment we can see strewn through our days upon the introduction of an incompetently designed ubiquitous technology. Accordingly, we should assert as a principle the idea that ubiquitous systems must not introduce undue complications into ordinary operations.

One should be able to open a window, place a book upon a shelf, or boil a kettle of water without being asked if one ‘really’ wants to do so, or having fine-grained control of the situation wrested away. One should not have to configure, manage or monitor the behaviour of a ubiquitous system intervening in these or similar situations—not, at least, after the very first time one uses it or brings it into some new context. Furthermore, in the absence of other information, the system’s default assumption must be that an adult, competent user knows and understands what he or she wants to achieve, and has accurately expressed that desire in his or her commands.

In short, one should not have to work many times as hard to achieve some utterly mundane effect (such as drawing a bath, starting a car or sharing contact information with a new acquaintance) in the presence of ubiquitous systems as one would have otherwise. Nor should one be forced to spend more time fixing the mess resulting from some momentary slip in a sequence of interactions than the entire process should normally have taken in the first place. This will occasionally approach the level of complexity Kindberg & Fox (2002) refer to as ‘AI-hard’. Nevertheless, we should insist on excluding...
ubiquitous systems from our everyday lives unless and until they are
demonstrably more respectful of our time than information technologies have
tended to be in the past.

(e) Ubiquitous systems must be deniable

Our last principle is perhaps the hardest to observe: ubiquitous systems must
offer users the ability to opt out, always and at any point.

Users should have the ability to simply say ‘no’, in other words. In private
space, at least, one should be able to shut down the ambient informatic overlay
and face no penalty other than being unable to take advantage of whatever
benefits it offered in the first place. This means, of course, that realistic
alternatives must exist.

If one still wants to use an ‘old-fashioned’ key to get into one’s house, and not
have to have a radiofrequency identification tag subcutaneously implanted in the
fleshy part of one’s hand, this option should be available. Should one want to pay
cash for purchases rather than ‘tapping and going’ with a touchless payment
card, that too should be possible. And if one wants to stop a networked bathtub
or running shoe or car in the middle of executing some sequence, so that one may
take over control, there should be nothing to stand in the way.

In public, at an absolute minimum, ubiquitous systems with surveillant
capacity must announce themselves as such, from safely beyond their field of
operation, in such a way that one can effectively evade them. The measure used
to alert users need not be anything more elaborate than the signs already seen in
ATM lobbies and other such locales, warning us that our image is being
captured, but such measures must exist.

3. Prospects for implementation: a precedent

One of the obvious difficulties with any set of principles such as these concerns
the matter of compliance—or, looked at another way, enforcement.

Can a large and heterogeneous population of developers reasonably be
expected to police themselves, to spend the extra time and effort necessary to
ensure that the ubiquitous systems they produce do not harm or unduly
embarrass us, waste our time, or otherwise infringe on our prerogatives?

Recent technological history offers some support for this optimistic scenario:
starting in 1998, a grassroots movement towards the so-called ‘Web standards’
on the part of independent developers forced the hand of industry giants such as
Microsoft and Netscape, over a relatively short period.

Within a very few years, every major browser had been brought into
compliance with the set of standards the activists had called for; the combination
of structural and presentational techniques the so-called ‘standardistas’ insisted
on is now considered a benchmark of responsible Web development. By
any measure, this would have to be considered a very successful example of
bottom–up pressure resulting in wholesale improvements to the shared
technological environment.

The standardistas, it must be said, were on the right side of an emerging
business calculus to begin with: by the time the standards movement came to
prominence, it was already punitively expensive for developers to code six or
seven different versions of a site, simply to render properly in all the incompatible browsers then popular. It is also true that they enjoyed the advantage of urging their changes on a relatively concentrated decision nexus, at least where the browser makers were concerned.

Ensuring that a given ubiquitous system respects our prerogatives will be many orders of magnitude more difficult than ascertaining whether or not a website complies with the relevant standards. The latter, after all, is something which can be verified by running a site’s source code through an automated validator. By contrast, we have seen how much room for interpretation there is in defining ‘undue complications’, let alone in determining what might constitute ‘harm’ or ‘embarrassment’. The grey areas are legion, compared with the simple, binary truths of Web standards, where either a site is coded in well-formed XHTML, or it is not. In the saga of Web standards, however, there is an object lesson in the power of bottom–up self-regulation to achieve ends in technological development which are both complex and broadly beneficial.

The prospect hinges on a simple clearly enunciated way for users and consumers to know when a system complies with the standards they wish to support. This would be a finding of fitness verified by an independent, transparent and international licensing body: a guarantee to all concerned that, to the degree possible, the system in question had been found to observe all necessary protections of the human user.

A mechanism such as this implies that, to some degree, we can feel more comfortable in allowing the market to regulate the adoption of ubiquitous systems, because that market will have been provided with accurate and appropriate information. A simple high-visibility binary marker will let users and consumers make informed decisions: either this system meets the standards as they existed at such-and-such a date or it does not. The full guidelines are of course there to peruse in detail should anyone wish to do so, but it is not necessary to have a comprehensive understanding of what they mean at the time of purchase, download or installation.

4. Conclusion

Clearly, no response to the inevitable downsides of a ubiquitous milieu will be anything close to perfect; even if we could assume for a second that all of the practical challenges posed by our embrace of ubiquitous systems were tractable, there will always be bad actors of one sort or another. Given the almost unlimited potential of such systems to facilitate the collection of all sorts of information, the extreme subtlety with which they can be deployed, and the notable propensity of certain parties—corporate, governmental—to indulge in overreaching information-gathering activities if once granted the technical wherewithal, abuses will certainly occur.

Barring deliberate malfeasance, though, I believe that many of the challenges we face can meaningfully be addressed by collective, voluntary means. If standards for the ethical and responsible development of everyday ubiquity, not necessarily the ones discussed here, can be agreed upon by a visible plurality of developers, the onus will be on others to comply with them.
Such provisions extend the possibility that we as users can meaningfully
— *educate* ourselves as to the nature of the various technologies grouped under
the rubric of ubiquitous computing;
— *decide* which of them we will invite into our lives, and under what
circumstances;
— *demand* that the technologies we are offered respect our claims to privacy, self-
determination and the quality of life; and
— (hardest of all) consistently *act* in accordance with our beliefs at work, at the
register and at the voting booth.

In an era in which an ever greater proportion of our daily activities are in some
wise shaped by the informational overlay enfolding them, and the ubiquitous
technical systems by way of which this overlay is made manifest, I believe that a
*laissez-faire* approach to such systems’ development is, to put it mildly, not likely
to lead to acceptable outcomes for the great majority of us. It is my hope that, by
enunciating a body of baseline expectations for their ethical and responsible
development, some progress can be made towards returning control of this
informatic environment to that person to whom it rightfully belongs: the
individual human user.

**References**

Arnall, T. 2005 *A graphic language for touch*. Oslo, Norway: AHO.


Marx, G. T. In preparation. Some conceptual issues in the study of borders and surveillance.