ETHICS AND INFORMATION TECHNOLOGY
VOL. 9
2007

SEIZING CONTROL?: THE EXPERIENCE CAPTURE EXPERIMENTS OF RINGLEY & MANN

Jane Bailey and Ian Kerr

Faculty of Law, Common Law Section, University of Ottawa, 57 Louis Pasteur St., Ottawa, ON, Canada K1N 6N5
E-mails: jbailey@uottawa.ca; iankerr@uottawa.ca

Abstract. Will the proliferation of devices that provide the continuous archival and retrieval of personal experiences (CARPE) improve control over, access to and the record of collective knowledge as Vannevar Bush once predicted with his futuristic *memex*? Or is it possible that their increasing ubiquity might pose fundamental risks to humanity, as Donald Norman contemplated in his investigation of an imaginary CARPE device he called the ''*Teddy*'' ? Through an examination of the webcam experiment of Jenni Ringley and the *EyeTap* experiments of Steve Mann, this article explores some of the social implications of CARPE. The authors' central claim is that focussing on notions of *individual* consent and control in assessing the privacy implications of CARPE while reflective of the *individualistic* conception of privacy that predominates western thinking, is nevertheless inadequate in terms of recognizing the effect of individual uptake of these kinds of technologies on the level of privacy we are all collectively entitled to expect. The authors urge that future analysis ought to take a broader approach that considers contextual factors affecting user groups and the possible limitations on our collective ability to control the social meanings associated with the subsequent distribution and use of personal images and experiences after they are captured and archived. The authors ultimately recommend an approach that takes into account the *collective impact* that CARPE technologies will have on privacy and identity formation and highlight aspects of that approach.

Key words: privacy, surveillance, personal experience capture, carpe, equality, webcamming, eyetap, glogging, Vannevar Bush, Jennicam, sousveillance, equiveillance, informed consent, reasonable expectation of privacy

Introduction

While the rest of North America was ringing-in 2004, JenniCam, the electronic eye providing the digital window into Jennifer Ringley's postmodern soul, briefly blinked and was then forever shut. From its inception in 1996, JenniCam provided interested viewers a continuous, uncensored glimpse into Ringley's home. Every aspect of her domestic life, from the mundane to her most intimate moments, was available over the web as a public offering consumed by anonymous viewers in the privacy of their own homes. By exploiting the potential inherent in the new technology, Ringley sought to challenge prevailing social conceptions of womanhood and the position of women within the public/private divide. While Ringley's live feed has now ceased, the online peepshows cobbled together from downloads and archived sexual excerpts caught by her webcam's once-unblinking eye are still available. As a result, the critical consciousness that informed Ringley's self-described ''social experiment'' has been co-opted into enduring vignettes of sexual objectification that, by robbing her documentary of its context, reinforce many of the messages she may have hoped to contradict.

During the same year that marked the cessation of Ringley's 7 years of relentless recording, the Association of Computing Machinery hosted an international workshop that would give new meaning to the phrase ''seize the day''. Aptly named ''CARPE'', the subject of the workshop was the ''Continuous Archival and Retrieval of Personal Experiences''. Inspired by the great vision of Vannevar Bush's futuristic *memex* (Bush 1945), leading researchers from across the globe gathered at Columbia University to investigate the manner in which the continuous archival paradigm fundamentally alters our relationship to biological memory. Professor Steve Mann, the workshop's keynote speaker, described an invention called *EyeTap*, a ''visual memory prosthetic'' that enables

Mann to continuously archive and retrieve his entire life by turning his eye into a camera and his body into a web server. In explaining the social implications of CARPE, Mann described his notion of ''equiveillance'': a state in which the watcher becomes the watched in a balance of countervailing images and perspectives. According to Mann, the ability to capture, archive, and retrieve one's personal experiences is a privacy-enhancing antidote to excessive state and private sector surveillance. Likening his *EyeTap* to the blackbox flight recorder in an airplane, Mann claimed that a first-person recording of an activity, where the person doing the recording is a participant, enhances public safety and provides participants with a means to counter traditional power structures. It provides an alternative documentary of events should disputes arise.

Though Mann has sought to distance himself from what he sees as the ''puerile'' focus of Ringley's on-line presence, the two share a profound sense of techno-optimism. Both seemed to cherish the *unblinking* gaze. Refusing to be defined by the intrusive and objectifying gaze of our surveillance based society, Ringley and Mann launched their own projects of self-definition by voluntarily adopting CARPE devices as an apparent means of social empowerment. Seizing control of the camera, Ringley and Mann attempted to influence how they are viewed, framing the image in ways that capture a more personal and more subjective truth. The new technology, ideally, offers a means of inverting the power dynamic. It allows individuals access to modes of image production previously beyond their reach. While the practices pioneered by Ringley and Mann allow more people to create more images, it is unclear what effect this will ultimately have on the surveillance society. In a world of ''equiveillance'' or, perhaps more precisely, *omni*veillance, how do we conceive of privacy and its role in identity formation and collective empowerment?

This article explores aspects of this question in four parts. ''*Eyetap* and Jennicam'' describes in greater detail the projects of Mann and Ringley, focussing on their visions of technological empowerment as a means of countering surveillance and challenging mainstream visions of femininity. ''The social promise of CARPE'' broadens the context to explore earlier visions of the social promise of CARPE technologies encapsulated in Bush's *memex* and Donald Norman's *Teddy*, (Norman 1992) focussing in particular on assumptions about control and privacy underlying those visions. ''In control'' relies on aspects of the Ringley and Mann experiments that problematize assumptions about personal control and its meaning in the context of CARPE. ''Beyond privacy through individual consent'' again relies on the Ringley and Mann experiments to cast into stark relief problems associated with the individualistic notion of privacy that are necessary to Bush's underlying argument as to the social value of these technologies, but appear to be antithetical to their use in meaningful individually and collectively empowering ways. The ''Conclusion'' draws together the insights about control and privacy gained through the explorations of *EyeTap* and Jennicam, urging further interrogation of the privacy and identity implications of CARPE technologies in the wake of ever-broadening online access to them.

Eyetap **and Jennicam**

Eyetap – the Steve Mann experiment

Since his childhood in the 1970s, Steve Mann has been building and wearing computer systems with the aim of generating electronically mediated vision. *EyeTap* is an ingenious wearable system that achieves this aim. Modifying light computationally, this device can be used to affect vision in various ways. It can be used to augment vision (e.g., seeing better in the dark), or to alter what is seen (e.g., filtering out unwanted advertising from one's visual field). It can also be used to correct optical disorders. Mann has described his multi-purpose device as an ''existential technology'' (Mann 2003); ''part of an iterative process of invention, design, building, using, and then back to reinvention, redesign, rebuilding, and re-using, and so on...'' (Mann 2004 at 1) Once bulky, cumbersome, eye-catching systems made of spare army surplus parts, over the years, *EyeTap* has morphed into more miniaturized personal imaging systems that are not only ''acceptable in terms of wearability and weight'' but also completely inconspicuous in terms of contemporary fashion (Mann 2004 at 3; Jardin 2005).

What started as a tool for altering visual experiences through mediated reality has since, quite serendipitously, taken on important features that have no analog in traditional eyewear. As Mann describes it,

> EyeTap eyeglasses can help us remember better, through what is called a lifeglog ... 'glog, for short. A 'glog uses lifelong video capture to record what our eyes see over our entire lifetime. By using the data management capabilities of modern computers, we will be able to recall things that we have seen with perfect clarity in a natural and intuitive way. Having an on-demand photographic memory can help all of us by offloading, to a

> wearable computer, the task of memorizing now-mundane details that might only later become important. This kind of visual memory prosthetic is very beneficial to all of us, since our environments have become so overloaded with information. This lifeglog can also be used to increase personal safety and crime reduction by providing visual evidence for criminal acts, and to allow for trusted third party inverse surveillance (''sousveillance'') in situations where the user may feel threatened. Moreover, in settings where surveillance already exists, sousveillance (the recording of an activity by a participant in the activity) can help prevent the surveillance recordings from being taken out of context. It is this contextual integrity of the evidence, combined with a personal right and responsibility of individuals to preserve evidence, that sets forth an equilibrium between surveillance and sousveillance. (Mann 2004 at 2)

While experimenting with various versions of *EyeTap* over a 20-year period and their means of technological empowerment, Mann regularly perceived himself as discriminated against whenever anyone realized that he was engaged in CARPE (Mann 2004; Mann and Niedzviecki 2001). Interestingly, he noticed that the discrimination seemed to correlate with the amount of surveillance in an immediate environment: the more surveillance there was in any given space, the more likely it seemed that he would suffer mistreatment for his participant-oriented sousveillance. Often, this led to interactions and sometimes altercationswith public and private authorities, causing Mann to value the record created by his CARPE activities and to propose what he calls the *equiveillance doctrine*:

> [a]lthough there may well be situations where sousveillance might be inappropriate, sousveillance must never be prohibited in situations where surveillance exists. (Mann 2004 at 10)

Believing that ''[t]he existence of surveillance takes away a reasonable expectation of privacy, and therefore creates, of a space, a free-fire zone'', Mann contends that people in that space have not only a right but perhaps even a responsibility to capture their own personal records of their lives in order to provide a proper context for what the surveillance data might show (Mann 2004). Consequently, he has encouraged and created an entire ''glogger'' community who do just that (Mann 2007).

Jennicam – the Jenni Ringley experiment

In 1996 Jennifer Ringley, a university student and resident of Washington DC, set up a working web camera in her bedroom (White 2006), which offered to the Internet-connected everywhere a regularly updated feed of her daily activities of living. One could see Ringley studying, eating, sleeping, grooming, and also gain information about health issues she underwent, and her sexual preference and activities (Gerrard 1997). The Jennicam operated in this fashion, free of charge, for several years until, as Ringley apparently explained it, it was necessary for her to charge a fee in order to maintain the equipment necessary to facilitate the live feed. Eventually, Ringley discontinued operation of the site after PayPal changed its rules relating to adult content and refused to support her site any longer (Ringley 2003). Ringley explained her site as ''a chronicle, a longterm experiment'' showing her life ''exactly as it would be whether or not there were cameras watching'' (Abreu 2003).

Despite her webcam's unblinking gaze, Ringley believed she maintained her privacy:

> I don't feel I'm giving up my privacy. Just because people can see me doesn't mean it affects me – I'm still alone in my room, no matter what. (Ringley 1998)

Further, she rejected assertions that her site constituted pornography, noting:

> Yes it contains nudity from time to time. Real life contains nudity. Yes it contains sexually explicit material from time to time. Real life contains sexual material. However, this is not a site about nudity and sexual material. It is a site about real life. (Ringley 1998)

Ringley may have been in control of the camera that captured and distributed the images of her initially, and in that way in control over the degree to which she waived her right to disconnect her publicly identifiable persona from her innermost thoughts, emotions and personal activities. However, once she made them available over the Internet, she forfeited significant control over the way in which the images were used, amended, elaborated upon and further distributed. What may have begun as an ''experiment'' depicting ''real life'', was all too easily dissected, compartmentalized and subverted into pornography produced by, and primarily for, men.

Paul Brown, for example, set up a website where he archived numerous shots from Jennicam, many of which feature Ringley's bed, often with full view of her naked buttocks and occasionally with her masturbating (Brown 2007). The Peeping Moe's website, a website ''for the voyeur of discriminating taste'', selected a seductive shot of Ringley in a lacy camisole for its fan page (Peeping Moe 2001). Yet another ''fan'', Howard Landman selected photos of Ringley (many in states of undress or seductive poses, even though most accounts of the website describe it as

largely mundane) and wrote parodies of ‘‘The Sonnets of Orpheus’’ to go with them (Landman 1996). Thus, even if Jenni Ringley did not start out to produce pornography, she eventually did star in it.

Common themes

Despite obvious differences, the CARPE experiments of Ringley and Mann raise numerous common themes. Both claim to have entered into largely passive, self-surveillance fully voluntarily. Their efforts to chronicle their ‘‘real life’’ existences were both experimental and yet purposive. Mann hoped to set the stage for self-empowerment through CARPE by offering the many advantages of mediated reality, serendipitously discovering that individuals can fight back against corporate and government surveillance by being equipped to surveil the surveillors. Ringley has suggested that, among other things, she hoped her chronicle would reveal more about the real life of a woman than was presented in mainstream media representations. The techno-optimism inherent in the documentary projects of Mann and Ringley parallels that of Vannevar Bush in his *memex*, while, at the same time, raising contemporary examples of the risks associated with CARPE highlighted in Donald Norman’s *Teddy*.

The social promise of CARPE

The Memex – Bush’s vision

Born to a pastor and the daughter of a banking family in Chelsea, Massachusetts in 1890 (Zachary 1999), Vannevar Bush went on to enjoy an illustrious career as a professor, scientist and thinker (Peterson 2006; Miller 1998). As Chair of the *Manhattan Project*, Bush was quite successful in convincing the U.S. government that scientists could and should play a powerful role in warfare (Lepkowski 1999); but, by 1945, Bush became deeply concerned with whether scientists would continue to serve any useful function in the post-WWII years. It was in that year that *Atlantic Monthly* published his now famous piece ‘‘As We May Think’’ (Bush 1945), in which he articulated ideas about associative indexing of knowledge credited as playing a seminal role in inspiring hypertext as we know it today (Berners-Lee 1995). (Interestingly, Bush had penned the letter upon which the manuscript was based some 6 years before the *Atlantic Monthly* publication [Nyce and Kahn 1991 at 51–56].)

Noting the role that science had played in creating communications technologies that were facilitating a seemingly ever-expanding record of research and discovery that allowed knowledge to endure beyond the life span of individual thinkers and inventors, Bush lamented the under-utilization of knowledge, which he attributed primarily to its organization into mechanistic categories. His post-WWII vision for scientists was in making the record of knowledge more complete, readily accessible and searchable by creating databanks of material organized through associations between material that better reflected human thought processes than did categorical indexing (Bush 1945).

Buoyed by discoveries relating to dry photography and miniaturization, among others, Bush envisioned scientists extending their individual memories (and thus expanding the knowledge available for inclusion into the common record of humanity) by wearing walnut-sized cameras that would enable them to continuously photograph scenes and images they deemed worthy of recording as they went about their day-to-day lives (Bush 1945 at 2). These and other materials would then be combined into a personal database that Bush termed a *memex*:

> A memex is a device in which an individual stores all his books, records, and communications, and which is mechanized so that it may be consulted with exceeding speed and flexibility. It is an enlarged intimate supplement to his memory. (Bush 1945 at 6)

The *memex* would allow individuals (Bush’s focus was on the scientific elite [Nyce and Kahn 1991]) to store significant quantities of information, but most importantly, to recall and organize them in combinations that would create new records from the existing ones, while at the same time documenting the associative trail that led to their combination. These individual records could be shared, culled and organized through association to create a common record:

> There is a new profession of trail blazers, those who find delight in the task of establishing useful trails through the enormous mass of the common record. The inheritance from the master becomes, not only his additions to the world’s record, but for his disciples the entire scaffolding by which they were erected. (Bush 1945 at 8)

Bush venerated technology’s ability to expand both the ability to create records, as well as to make them more widely available and more easily accessed. His vision of the memex built upon those abilities, pushing toward better mechanisms for organizing and sorting the records created. Bush’s 1945 vision is relatively untempered by critical

reflection – there is little discussion of any potential downsides of this widespread documentation and sorting process. With the benefit of the passage of time and building on the social experiences made possible by advances in and the proliferation of computing and communications technologies such as hypertext and the Internet, in 1992, Northwestern University professor Donald Norman offered a perspective of CARPE that more carefully contemplated some of its broader social implications. He did so using an imaginary device, known as the *Teddy* (Norman 1992).

The Teddy – Norman's vision

In his book, *Turn Signals Are the Facial Expression of Automobiles* (Norman 1992), Norman envisioned the *Teddy* – a personal computing device that would serve, among other things, to allow individuals to move beyond the limitations of the human memory. Noting that technology had both expanded humans' ability to create and access information, while at the same time imposing progressively greater data retention requirements in order to access and interact with that information, Norman invited readers to imagine fighting the demands of technology with further technology:

> [S]ociety has evolved to the point where everyone always carries a portable computer with them, except it isn't thought of as a computer, it is thought of as a personal, confidential assistant.
> ...
> Teddys would be with their user for their entire lives. ... As a result, Teddy would always retain a complete record of all the person's personal experiences and knowledge for an entire lifetime even as it changed in physical form. (Norman 1992 at 74)

Although a self-declared techno-optimist, Norman was clearly cognizant of some of the risks associated with these technologies when considered within the broader social, legal and psychological context. Socially, Norman recognized the privacy concerns related to the *Teddy* – the possibility that our innermost thoughts and experiences would be too readily accessible to others, but envisioned futuristically sound encryption systems as the primary mechanism for addressing privacy concerns (Norman 1992 at 76). Norman also predicted the possibility of legislative intervention – either to require people not to record information in certain situations, or perhaps more ominously, to require them to keep recording at all times (Norman 1992 at 76). Finally, Norman asked questions about the psychological implications of being tethered to one's technology and suggested that the *Teddy*'s ongoing reinforcement or questioning of its ''owner's'' thoughts and feelings raised the potential for an increasingly tuned-out, delusional (or conversely paranoid) population, incapable of the invention and creativity made possible through quiet, reflective alone-time (Norman 1992 at 79–80).

While expressing lingering doubts about the double-edged sword of technology, Norman queried:

> What I want is all of the virtues of machines and none of the disadvantages – the scientific version of eating my cake and having it too. After all, if I carried my own information bank, my own Teddy with me at all times, with me in control of the on-off switch, what are the deficits? (Norman 1992 at 84)

While Norman seems to have satisfied himself that consent and an on-off switch are sufficient to create a win–win situation, (not unlike many policy-makers in our current debates about RFID and other sensor networks) [OIPC Guidelines for RFID 2006] it is our contention that some of Norman's other concerns set out above are in fact very well-placed and merit further investigation. In ''In control'' and ''Beyond privacy through individual consent'' we focus on two aspects of that investigation in the context of the Ringley and Mann experiments: (i) the degree to which one can ever be said to be ''in control'' of the technology and, (ii) the adequacy of individualized notions of privacy (whether through technological mechanisms like those envisioned by Norman or through legal mechanisms such as ''consent'').

''In control''?

Central to both Bush and Norman's visions of CARPE technologies is either a presumption, or at least a wish, for individual control over the devices and their product. All else being equal, individual control might well prove determinative in the quest for individual and collective empowerment through these technologies. Unfortunately, the reality is that these technologies exist in a context where all else *is not* equal – where forces such as prejudice, sexism, market power, and state coercion all operate to undermine the ability for all netizens to enjoy control equally, if at all. The inequalities resulting from these social forces are graphically demonstrated by the experiments of Ringley and Mann, both of whom have expressed hope that their CARPE experiments would prove to be socially empowering and equality enhancing, both for them and for others.

For her part, Ringley has suggested that one aspect of her experiment was to challenge mainstream, unrealistic Hollywood depictions of what it means to be a woman and of how women live. In that regard, she stated:

> I just want to show people that what we see on TV – people with perfect hair, perfect friends, perfect lives – is not reality. I am. (Senft 2005 at 12)

Likewise, Mann has expressed hope that CARPE devices will increase people's sense of control over their environments in an age of increasing corporate and government surveillance:

> In affording all people to be simultaneously master and subject of the gaze, wearable computing devices offer a new voice in the usually one-sided dialogue of surveillance. They suggest a way towards a self-empowering sousveillance for people as they traverse their multiple and complex networks. (Mann et al. 2003 at 338)

Like Bush and Norman, both Ringley and Mann envision *memex* and *Teddy*-like technologies to be instruments of potential empowerment – empowerment to break free from sexist stereotypes in Ringley's case and empowerment to counterbalance the ubiquity of corporate and government surveillance in Mann's case.

On closer inspection, however, there are many reasons to be concerned that CARPE devices may not live up to their perceived potential. These devices do not operate in a social vacuum. The intended records of the participants are impacted by: (i) the force of law (ii) the actions of other people, (iii) technological design, and (iv) private sector contracts governing the use of these technologies (and the records that they produce). Each of these social forces has the potential to undermine both individual control over the technology itself, and also the ability to convey empowering messages like those hoped for by Ringley and Mann.

First, in the context of the law, Norman himself predicted the possibility that legal restrictions might be placed on an individual's ability to control the technology – either to turn it on or to turn it off (Norman 1992 at 76). As authorities become increasingly aware of the information available within personal records, as well as circulating more generally on the Internet, there is likely to be a keen interest in legal involvement with the process of creating, maintaining and gaining access to those records (Kerr and Mann 2006). And it is becoming less difficult for law enforcement agencies to do so. For example, worldwide responses to the Council of Europe's *Convention on Cybercrime* have resulted in the adoption of legislation in many jurisdictions that would require all telecommunications service providers to build a global intercept capability into all telecommunications infrastructures, thus allowing a 'backdoor' for designated officers to gain access to electronic communications and other stored electronic records (Gilbert et al. 2006). In this context, CARPE devices are like a black box with a peep hole.

Second, the Ringley experiment highlights other people's impact on control over CARPE. Despite Ringley's stated intention to counter mainstream representations of women, the nature of the digitized online content of her record permits others to 'mashup' and thereby seize control of her original message. Numerous examples abound, from The Peeping Moe's selection of a partially clad Ringley for their website, to Howard Landman's selection of what he described as ''R-rated'' and ''maybe'' ''X-rated'' images of Ringley from a multitude of mundane images as the subject of many of his ''Sonnets to Jennicam (Landman 1996). As a result, while Ringley endeavoured to capture the entirety of her experience as a woman, others were able through cutting, pasting, remixing and mashing, to convey a very different message than the one she had intended – usurping control over her social experiment for change in favour of tired and time-worn reiterations of female sexual objectification.

Third, the technologies themselves are often designed to play a significant role in terms of control over CARPE. The proliferation of self-documenting technologies like *My Space*, *Deja View*, *Eyeblog*, *Lifestreams*, *My LifeBits* and *Total Recall* have become increasingly sophisticated systems, some of which are sure to adopt digital rights management systems (DRMs). DRMs often invoke technological protection measures (TPMs), software programs that make it difficult or impossible for most individuals to access, manage or even know about various layers of personal information collected by the devices concurrent in this case with personal experience capture.

Fourth, the level of control that an individual has over these devices can be further diminished when DRMs contain a one-sided, standard form *End User Licence Agreement* (EULA) through which corporations (or governments) are able to assert a further level of control over users' records. If, for example, individuals' CARPE devices required a web interface while staying at a Hilton hotel, the hotel EULA is likely to specify that, among other things, any information released during the interface constitutes the trackable, collectable, compilable and resaleable property of the corporation, across the universe and in perpetuity (Foster 2005).

Each of the four social factors set out above help to highlight the tenuous and potentially fleeting nature of individual control over CARPE records. When one takes these into consideration, there are many reasons to be concerned that the technologies Bush and Norman envisioned as potentially empowering for humankind could, just as easily, be used to assert unprecedented levels of control over individuals and their information. Even though these devices do create some new forms of individual control, serious questions remain about their overall impact. These are double-edged digital swords. At the same time that they create new possibilities for individuals, CARPE devices also result in individual waivers of various other forms of social power and control; losses of power and control that can have a negative impact not only on the individuals said to waive them but also on the collective value of privacy. Some of these are addressed in ''Beyond privacy through individual consent''.

Beyond privacy through individual consent

Norman's *Teddy* suggests a vision of the world where, as long as each individual is in control of his or her CARPE device and encryption systems are adequate, privacy concerns are alleviated. Individuals are able to assert control (or to consent to waive control) over their information. It is simply a matter of individual choice. Individualistic analyses of this kind are not only common but tend to predominate thinking about whether any genuine privacy issues arise from CARPE – including the experiments of Ringley and Mann (Senft 2005; Mann and Niedzviecki 2001). Indeed, this approach to privacy as an individual right and a producer of individual goods is paradigmatic of the literature in the West on privacy theory. As Bennett and Raab (2006, p. 14) have aptly noted:

> The privacy paradigm rests on a conception of society as comprising relatively autonomous individuals. It rests on an atomistic conception of society; the community is no more than the sum total of the individuals that make it up. Further, it rests on notions of differences between the privacy claims and interests of different individuals. Individuals, with their liberty, autonomy, rationality, and privacy, are assumed to know their interests, and should be allowed a private sphere untouched by others.

This paradigm has been applied to Ringley and Mann as follows. Ringley's image is hers, as is the personal space of her home. As a consenting adult, she can decide to waive any privacy in relation to her image or her personal space by broadcasting it, allowing it to be archived, retrieved, copied and morphed. She can surrender what many might consider to be ''private'' aspects of her life to the public domain (Senft 2005; Jimroglou 1999).

In Mann's case, he himself justifies his *EyeTap*, in part, on the basis that it offers a form of negotiation between individuals that is not possible in the case of corporation or government surveillance (Mann 2004). In the context of ''sousveillance'' that is streamed in realtime to the Internet, Mann has consented to waive his expectation of privacy in the digital images that document his daily experiences and his ''subjects'' can negotiate with him if they do not wish to consent to his incorporation of their images and actions into his own record (Mann 2004; Mann and Niedzviecki 2001).

It is our contention that an analysis, which reduces all privacy interests to nothing more than an individualistic series of waivers and consents is wholly unreflective of broader social privacy concerns raised by ubiquitous CARPE. Before addressing these concerns, however, we also wish to point out that even if one accepts the idea that individual ''consent'' is sufficient to address privacy concerns raised by these technologies, very serious questions arise about the necessary conditions under which these individual cedings can be said to truly reflect *informed* consent.

''Informed'' consent

The concept of informed consent is foundational to the waiver of basic rights such as: privacy, the right to counsel and the right to be secure against unreasonable search and seizure in various legal systems, including Canada. Whether informed consent will be found to have been given rests upon a contextual analysis of numerous factors including the seriousness of the right being waived, the seriousness of the effect of the waiver, the alleged consentor's knowledge of the right alleged to have been waived and of the consequences of the waiver in the circumstances. The Supreme Court of Canada in *R. v. Borden*, [1994] 3 S.C.R. 145 encapsulated the analysis as follows at para. 34:

> ...A right to choose [to waive a protected right] requires not only the volition to prefer one option over another, but also sufficient available information to make the preference meaningful.

Even proceeding from the paradigmatically individualistic approach to privacy theory inherent within an analysis of informed consent and waiver, questions about the validity of the ‘‘consent’’ to waive privacy raised by CARPE immediately surface. In a world where *memex* and *Teddy*-like technologies already exist, it is essential to think through the kinds of factors that ought to be considered necessary in order to be convinced that a meaningful, volitional choice to waive individual privacy has been made. The Ringley and Mann experiments raise some of those questions directly.

When Jenni Ringley plugged in, did she actually understand that she was waiving her privacy or the significance of the effect of that waiver? Since she has suggested that she did not consider her privacy to have been interfered with (Ringley 1998), it would seem that she did not. Could she have reasonably been expected to anticipate not just the viewing and capturing of some of her most intimate moments by complete strangers, but also the re-mixing and re-distribution of significant aspects of her life to millions of people by individuals like Landman? While it seems we can almost certainly be satisfied that she freely preferred the option of distributing the record of her life on-line, when she made that decision she very likely *did not* grasp the long-term consequences of the permanent distribution of her image or its re-mixing (to focus on the relatively few occasions when her record included explicit displays of sexual activity). These considerations are crucial to an analysis of informed consent, even in an individualistic account of privacy.

In the Mann context, even if we are to accept that, with his extensive technological knowledge, he meaningfully waived his own right to privacy, what about the would-be targets caught in the crossfire of the capture of his experiences? Even if Mann had negotiated individually with every would-be target before capturing their image in his record, what exactly could they be said to have consented to? What would they need to know in order to be said to have reasonably understood the nature of his experiment and the scope of the intended use of their image and activity? What if they had consented to collection, use or disclosure for one purpose but Mann later decided to apply it to some other purpose? What if Mann conformed with his originally disclosed purpose but made his experiences publicly available so that others are able to collect, use or disclose it as they see fit? Practically speaking, Mann’s ‘‘negotiations’’ are unworkable on an informed consent model. Precisely for this reason, Canada’s private sector privacy laws generally require the ability of a data subject to withdraw consent at any time. [*PIPEDA* Sched. 1, principle 4.3.8]

These issues will continue to take on renewed significance as more and more *memex* and *Teddy*-like technologies begin to proliferate and the terms of their use are governed by standard form click wrap agreements. When individuals using *My Life Bits* click ‘‘I agree’’ to the so-called privacy terms set by MicroSoft in its EULA, they are bound to have even less control over the capture, archival and retrieval of their experiences than Mann who, as inventor, has the luxury of setting his own terms of use. Even less control is experienced by those who find their way within the strange digital *mise en scene* of the lives of those whose CARPE devices surround them in public spaces. Given the pace of technological implementation and adoption, it is hard to imagine that most people will truly understand the nature of what they are said to be consenting to by walking into public spaces. Worse still are the implications when EULA-enerated security holes and other computer attacks open-up the black boxes of their lives to the world wide web.

As difficult as these questions seem to be, for the purposes of advancing our argument let us presume that we could collectively devise meaningful ways to assess whether there has been informed consent to waive privacy in relation to CARPE. In our view, focussing the analysis of the privacy implications of these technologies on consenting individuals misses the collective, social value of privacy and the degree to which even individually valid cedings of ‘‘privacy’’ affect the collective good. We suggest that one fruitful avenue for future exploration in this regard is to consider the implications of the way in which common law courts in many parts of the world have tended to connect each individual’s expectation of privacy (with respect to particular spaces and information) with the collective assessment of whether that expectation is reasonable having regard for surrounding aspects of social context.

Privacy as a collective value

In Canada and the United States, for example, although privacy is addressed in law as an individual right (usually against *state* intrusion), the degree of privacy to which an individual is entitled is premised upon whether their expectation of privacy was reasonable in the circumstances. [*R. v. Tessling* (2004) 3 S.C.R. 432; *U.S. v. Kyllo* 533 U.S. 27 (2001).] Here, the analysis tends to appeal to a somewhat ephemeral, collectively defined standard in order

to determine whether an individual's subjective expectation of privacy in relation to a particular space or piece of information, was ''objectively'' reasonable. This approach adopts certain widely accepted, but largely unspoken social norms, a kind of *collective* ''wisdom'' about what kind of spaces and information are ''private'' and what sort of uses can be made of them. In this way, what privacy any individual is entitled to expect by law depends upon how that expectation compares to some collectively defined norm.

How will that collectively defined norm be reshaped as an exponentially increasing number of ''consensual'' individual cedings continue to mount with the uptake of more and more CARPE devices? While the otherwise private experiences that Ringley or Mann might choose to cede as individuals may, on their own, have little impact on the collective reasonable expectation standard, Internet technologies tend to exhibit a ''long tail'' effect (Anderson 2006). One might therefore expect that the individual cedings of thousands or millions of personal experience capturers, collecting, archiving, retrieving, and in some cases streaming images or soundbytes from wherever they may be, sometimes attracting hundreds of thousands or millions of hits per day, will, without anyone's say-so, eventually take their toll on the evaluation of the reasonableness of others' expectations of privacy in those spaces.

With respect to spatial privacy, Jennicam has been lauded for exploding the mythical divide between private and public – a notional division that undoubtedly has been used as a means to explain and justify discriminatory gender stratification – putting women in their ''private'' space in the home in order to leave public life to men (Senft 2005; Jimroglou 1999; Blair and Takayoshi 1997). Perhaps the collective impact of thousands of individual waivers over some notion of the ''private sphere'' could empower women by flouting a construct traditionally used to confine them. On the other hand, to the extent that what is played out in the home simply mirrors back or can be easily mashed-up to mirror back, replay, and reinforce the mainstream notion of woman as sex object – to de-contextualize all of the components that comprise one woman's life – CARPE's ultimate effect may well be to undermine the feminist point set out to be articulated.

Likewise with Mann's *EyeTap*, which risks undermining the effectiveness of his ''sousveillance'' project the moment that *EyeTap*-type devices are adopted *en masse* by police, government agencies and private security companies (the question is surely ''when?'' and *not* ''if''). As well, even if one weren't concerned about the glogger community's individual cedings of various aspects of their own privacy, there is still reason to be concerned about the degree to which glogging technologies limit or even undermine the ability of those caught in the crossfire to maintain a degree of privacy in public spaces – especially as more and more people are interested in wearing such devices or joining such communities. Although many people may accept the idea that what they do in a public space cannot be understood as confidential or private (since their actions can be seen by anyone sharing the space), it is our contention that when personal experiences are continuously capturable, archiveable, retrievable, mashable and streamable, we are presented with various qualitative differences in terms of the level of personal intrusiveness – regardless of whether these possibilities rest in the hands of government, corporations or individuals like Steve Mann.

Recognition that individual uptake of privacy-ceding technologies such as CARPE may affect our social and legal concepts as to the privacy available not just for those who choose to adopt these technologies, but also for all citizens collectively is simply the first step in recognizing the need for further investigation and development of an understanding of the social dimensions of privacy. As Priscilla Regan (1999, p. 221) noted in the context of rising concerns relating to dataveillance technologies:

> Most privacy scholars emphasize that the individual is better off if privacy exists; I argue that society is better of as well when privacy exists. I maintain that privacy serves not just individual interests but also common, public and collective purposes. If privacy became less important to one individual in one particular context, or even to several individuals in several contexts, it would still be important as a value because it serves other crucial functions beyond those that it performs for a particular individual. Even if the individual interests in privacy became less compelling, social interests in privacy might remain.

Conclusion

More than six decades have passed since Bush first gave us his *memex* and articulated with unguarded optimism the value that postwar scientists and the not-yet-burgeoning field of information technology might offer to society. As CARPE technologies and experiments such as those of Ringley and Mann finally begin to proliferate, it is suggested that we would do well to pause to consider their implications–*collectively*. In this article, we have tried to

demonstrate why a more collective approach to investigating the social implications of the *memex* and other CARPE devices is necessary when evaluating their potential, particularly if we are to be convinced that they have the ability to empower individuals by enhancing privacy and identity formation. And if we are to maintain some level of commitment to privacy for society writ large in the face of ubiquitous, CARPE devices, then, in our view, it is essential to transcend the standard analyses of individual control and consent. As such, it is toward a more developed understanding of the social or collective dimensions of privacy that privacy theorists must turn their focus.

Acknowledgments

The authors wish to acknowledge and thank Katie Black, Jeremy Hessing-Lewis, Louisa Garib, Brad Jenkins and Julie Shugarman for their invaluable research and editorial assistance, as well as the Social Sciences and Humanities Research Council for funding *On the Identity Trail*, a four year research project from which this article derives. Special thanks also to our colleague Steve Mann for spurring us on with truly stunning and original ideas, as always, inspiring much shock and awe.

References

E. Abreu. Voyeur Web Site JenniCam to go Dark After 7 Years. Online at http://www.boston.com/ae/celebrity/articles/2003/12/10/voyeur_web_site_jennicam_to_go_dark_after_7_years/ accessed 01.15.2007, 2003.

C. Anderson. *The Long Tail: Why the Future of Business is Selling Less of More*. Hyperion Press, 2006.

T. Berners-Lee. Hypertext and Our Collective Destiny. Online at http://www.w3.org/Talks/9510_Bush/Talk.html accessed 01.16.2007, 1995.

C. Bennett and C. Raab, The *Governance of Privacy: Policy Instruments in Global Perspective*. The MIT Press, Massachusetts, 2006.

K. Blair and P. Takayoshi. Navigating the Image of Woman Online. Online at http://english/ttu.edu/kairos/2.2/coverwebe/invited/kb.html accessed 01.16.2007, 1997.

P. Brown. Jennicam: Last Week at Jenni's Place. Online at http://www.arttech.ab.ca/pbrown/jenni/jenni.html accessed 01.15.2007, 2007.

V. Bush. As We May Think. *The Atlantic Monthly*, July: 1–8, 1945.

E. Foster. History Writ Small. Online at http://www.infoworld.com/weblog/foster/2005/02/10.html accessed 01.16.2007, 2005.

L. Gerrard. Thoughts on Computers, Gender, and the Body Electric. Online at http://english.ttu.edu/kairos/2.2/coverweb/invted/lg.html accessed 01.15.2007, 1997.

D. Gilbert, I. Kerr and J. McGill. The Medium and the Message: Personal Privacy and the Forced Marriage of Police and Telecommunications Providers. *Criminal Law Quarterly*, 54(4): 469–507, 2006.

X. Jardin. Fancy Meets Function on Runway, Wired News (5 August). Online at http://www.wired.com/news/culture/0,1284,68432,00.html accessed 01.15.30, 2005.

K. Jimroglou. A Camera With a View: JenniCAM, Visual Representation, and Cyborg Subjectivity. *Information, Communications and Society*, 2(4): 439–453, 1999.

I. Kerr and S. Mann. Exploring Equiveillance. Online at http://www.anonequity.org/weblog/archives/2006/01/exploring_equiv_1.php accessed 01.16.2007, 2006.

H. Landman. The Sonnets to Jennicam. Online at http://www.polyamory.org/_howard/Jenni/ accessed 01.16.2007, 1996.

W. Lepkowski. What did Vannevar Bush Really Do? *Chemical & Engineering News*, 77(3): 43–47, 1999.

S. Mann. Existential Technology: Wearable Computing is Not the Real Issue! Leonardo. *MIT Press Journals*, 36(1): 19–25, 2003. Online at http://www.eyetap.org/papers/docs/id_leonardo_36_1_19_0.pdf accessed 01.31.07.

S. Mann. Continuous Lifelong Capture of Personal Experience with EyeTap in Proceedings of the 1st ACM Workshop on Continuous Archival and Retrieval of Personal Experiences (CARPE 2004). Online at http://www.eyetap.org/papers/docs/p1-mann/, 2004.

S. Mann. Online at http://wearcam.org/glogs.htm acessed 31.01.07, 2007.

S. Mann and H. Niedzviecki. *CYBORG: Digital Destiny and Human Possibility in the Age of the Wearable Computer*. Doubleday Canada, 2001.

S. Mann, J. Nolan, and B. Wellman. Sousveillance: Inventing and Using Wearable Computing Devices for Data Collection in Surveillance Environments. *Surveillance & Society*, 1(3): 331–355, 2003. Online at http://www.eyetap.org/papers/docs/sousveillance.pdf accessed 01.31.07.

C. Miller. Learning from History: World War II and the Culture of High Technology. *Journal of Business and Technical Communication*, 12: 288–295, 1998.

D. Norman. *Turn Signals are the Facial Expression of Automobiles*. Perseus Publishing, c. 6, 1992.

J. Nyce and P. Kahn, editors. From Memex to Hypertext. Academic Press Inc., 1991.

Ontario Information and Privacy Commissioner. Privacy Guidelines for RFID Information Systems (RFID Privacy Guidelines). Online at http://www.ipc.on.ca/images/Resources/up-rfidgdlines.pdf acessed 01.31.2007, 2006.

Peeping Moe Website. Online at http://web.archive.org/web/20010309025939/http://www.peepingmoe.com/netcams/jennicam/jenni-fan-home.html accessed 01.16.2007, 2001.

T. Peterson. Memex Forges An Early Link. *Computerworld*, 40: 30, 2006.

Personal Information Protection and Electronic Documents Act (PIPEDA). Schedule 1, Principle 4.3.8. Online at http://laws.justice.gc.ca/en/showdoc/cs/P-8.6/bo-ga:l_1-gb:l_4//en#anchorbo-ga:l_1-gb:l_4 accessed 01.31.2007, c. 5, 2000.

P. Regan, *Legislating Privacy*. University of North Carolina Press, Chapel Hill, 1995.

J. Ringley. Frequently Asked Questions (14 May 2003). Online at http://webarchive.org/web/19980514225722/jennicam.org/faq/jenni.html accessed 01.15.2007, 1998.

J. Ringley. Notice (27 December 2003). Online at http://web.archive.org/web/19980514225722/jennicam.org/faq/jenni.html, 2003.

T. Senft. Camgirls*: Webcams, Live Journals and the Personal as Political in the Age of the Global Brand*. Ph.D. Dissertation, Department of Performance Studies, NYU, 2005.

M. White. *The Body and the Screen: Theories of Internet Spectatorship*. The MIT Press, 2006.

G.P. Zachary. Endless *Frontier: Vannevar Bush, Engineer of the American Century*. MIT Press, c. 1, 1999.