Patterns of surveillance – Lit Review

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
This article addresses the question of whether personal surveillance on the world wide web is different in nature and intensity from that in the offline world (Bennett, 2001, abstract).	The article presents a profile of the ways in which privacy problems were framed and addressed in the 1970s and 1990s (Bennett, 2001, abstract).	Based on an analysis of privacy news stories from 1999-2000, it then presents a typology of the kinds of surveillance practices that have emerged as a result of Internet communications (Bennett, 2001, abstract).	The article offers some tentative conclusions about the progressive latency of tracking devices, about the complexity created by multi-sourcing, about the robustness of clickstream data, and about the erosion of the distinction between the monitor and the monitored (Bennett, 2001, abstract).	These trends emphasize the need to reject analysis that frames our understanding of Internet surveillance in terms of its "impact" on society (Bennett, 2001, abstract).
Has the Internet changed the nature of personal surveillance? (Bennett, 2001, p.197).	The typical "privacy problem" that arose in advanced industrial states in the year 1970 had the following characteristics: • The problem most likely stemmed from an agency of the state. (Big Brother) • Surveillance would most likely arise from within the boundaries of the state	Five practices are discussed and illustrated: surveillance by glitch, surveillance by default, surveillance by design, surveillance by possession, and surveillance by subject (Bennett, 2001, abstract).	Eighty four percent of Internet users surveyed by the Pew "Internet & American Life project" in 2000 expressed fear that web sites will obtain personal information without their knowledge (Bennett, 2001, p.197).	Rather the Internet should be regarded as a "form of life" whose evolving structure becomes embedded in human consciousness and social practice, and whose architecture embodies an inherent valence that is gradually shifting away from the assumptions of anonymity upon which the Internet was originally designed (Bennett, 2001, abstract).

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
	- Surveillance practices were more visible to the data subject (with few exceptions the individual was aware when information was being collected about him or her, by whom and for what purpose) - Surveillance systems were discrete and bounded: the concept of the "databank" expressed a technological and political reality that personal information systems had some clear boundaries (Bennett, 2001, p.198).			
Are the privacy problems in the online	Thus, in 1970 the metaphor was "Big	I present a typology of the types of surveillance	Internet users want to know what web sites do	It is now commonplace to assert that privacy is

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
world qualitatively and quantitatively different from those in the offline world? (Bennett, 2001, p.197).	Brother" and the surveillance potential of the Orwellian state (Bennett, 2001, p.198).	that seem to have emerged on the world wide web, illustrated by examples from various recent privacy scandals (Bennett, 2001, p.197).	with their personal information, before they do it (Bennett, 2001, p.197).	becoming a very significant political issue (Bennett, 2001, p.197).
A charitable interpretation of these three examples would emphasize the socially beneficial uses of these tracking devices, in which the monitoring of individual behaviour online is an unintended consequence of a search for greater network speed and efficiency (Bennett, 2001, p.201).	Books were written emphasizing the dangers of the "databank" in response to a variety of government projects for the integration of personal information systems (4 as cited by Bennett, 2001, p.198). Twenty years later, it was apparent that the privacy issue had shifted in some significant ways (Bennett, 2001, p.198).	Larger law enforcement surveillance such as the FBI's hotly debated "Project Carnivore" are also outside of the scope of the paper (Bennett, 2001, p.198).	Eighty-six percent of the internet users favor "opt-in" policies requiring companies to get permission from users before any of their personal information is shared with third parties (Bennett, 2001, p.197).	It is high on the political agendas of advanced industrial states and many political candidates have been forced to develop positions on the subject (Bennett, 2001, p.197).
The privacy implications of examples such as these are generally never contemplated in the design and development stage of the product (Bennett, 2001, p.201).	Around 1990, the profile of the problem had assumed some rather different characteristics • Surveillance was just as likely to stem from the private sector as	Capture and manipulation of large quantities of personal information on individuals (Bennett, 2001, p.198).	I focus on the role of the individual as a consumer, rather than that of employee (Bennett, 2001, p.198).	To a significant extent, this heightened concern has been brough about by fears of how the Internet can track information on individuals without their knowledge or consent (Bennett, 2001, p.197).

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
Or if they are considered, they are considered the equivalent of "security" (Bennett, 2001, p.201). Once the product is released, the company is surprised by the intensity of the backlash and is forced to defend and perhaps withdraw its product (Bennett, 2001, p.201).	from government agencies • Surveillance assumed an international character • Surveillance was becoming more surreptitious (kept secret, especially because it would not be approved of) (Bennett, 2001, p.198).			
Surveillance by design In these instances, the assumption is that a certain level of monitoring online and offline is in the individual's interests, because it is good for you to be told about products and services that might make your life happier and more fulfilling and which you would otherwise not	By the 1990s, therefore, surveillance occurred as part of one's routine engagement with the public and private institutions of modern society (5 as cited by Bennett, 2001, p.198).	What then are the kinds of privacy problems that have arisen so far on this new medium, and how do they compare with those of the past? (Bennett, 2001, p.199). I have categorized these problems into a five-fold framework: • Surveillance by glitch • Surveillance by default	The metaphor of Big Brother was gradually replaced with that of the "data trail" left as individuals unwittingly engage in everyday and innocent activities (Bennett, 2001, p.198).	At the same time, a Harris interactive survey found that, out of a list of eight public policy issues, 56 percent of adults responded that they are "very concerned" about a loss of personal privacy (Bennett, 2001, p.197).

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
learn about (Bennett, 2001, p.201).		• Surveillance by design • Surveillance by possession • Surveillance by subject (Bennett, 2001, p.199).		
In these cases, the online monitoring of online behaviour is not shielded by other motivations (Bennett, 2001, p.201).	It is worth reflecting that the technical breakthroughs that have produced this remarkable transformation in human communications are barely more than a decade old (6 as cited by Bennett, 2001, p.198-199).	**Surveillance by glitch** Defined by the phenomenon of the "privacy glitch" or the "security breach" (Bennett, 2001, p.199). -cases are caused by human and/or technical error (Bennett, 2001, p.199). - account for tax records found in garbage dumps and medical records on remote beaches (Bennett, 2001, p.199). These are usually followed by a frantic period of damage control during which the organization tries to fix the problem, reassure the its users, and	The Internet is a distributed packet-based network; there are many gatekeepers and no authority. And it is interoperable (Bennett, 2001, p.199).	The category was ranked second only to education, of which 58 percent said they were very concerned and ahead of topics such as health care (54 percent), crime (54 percent) and taxes (52 percent) (2 as cited by Bennett, 2001, p.197).

Patterns of surveillance – Lit Review

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
		minimize embarrassment (Bennett, 2001, p.199).		
	The characteristics of this medium are unprecedented (Bennett, 2001, p.199). It allows many to many interactivity, or access from all sites to all sites (Bennett, 2001, p.199).	**Surveillance by default** A second category of concern stems from the unintended surveillance consequences of applications introduced for seemingly benign and worthy purposes (Bennett, 2001, p.199).	As a result of key decisions made a key times, the balkanization of the network was avoided. The Internet is open to all-comers (7 as cited by Bennett, 2001, p.199).	Privacy is a notoriously nebulous and subjective concept (Bennett, 2001, p.198).
	It is entirely digital, which means flexibility: digital information can be replicated and manipulated in graphics, text or video format (Bennett, 2001, p.199).	**Surveillance by default** A second category of concern stems from the unintended surveillance consequences of applications introduced for seemingly benign and worthy purposes (Bennett, 2001, p.200).	**Surveillance by default** It is often impossible to assign responsibility and determine motives within complex organizations (Bennett, 2001, p.200).	The nature of the privacy problem has shifted considerably since computer technology first became used in a wide-spread manner in the 1960s and the individuals began to raise concerns about how personal information was being collected, processed and disseminated by large public and private organizations using the latest information technology (Bennett, 2001, p.198).

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
		Surveillance by default and surveillance by design may have few differences in practice and effect (Bennett, 2001, p.201).	But these examples also illustrate the fine line between the intentional and the unintentional tracking of personal behaviour (Bennett, 2001, p.201).	Privacy had been on the agendas of the Organizations Economic Cooperation and Development, the Council of Europe, the European Community and to a lesser extent, the United Nations, since the late 1970s (Bennett, 2001, p.198).
		The initial manifestation of online surveillance is captured by the practice of spam e-mailing (Bennett, 2001, p.201).	To a large extent, however, the relationship between the unsolicited e-mails received by an individual and that individual's preferences and attitudes is very low (Bennett, 2001, p.201).	The growing involvement of international organizations reflected the realization that privacy was only partially a national problem amendable to resolution through national states agencies (Bennett, 2001, p.198).
		Most spam originates from scavenger software that gathers e-mail addresses (good and bad) from every corner of the web. Particularly susceptible are those who post their addresses	Even though spam e-mail, by some estimates, now constitutes anywhere up to 15% of all messages send over the web, it is still a very unsophisticated method of advertising as it is	**Surveillance by default** These cases have in common a set of unintended, and perhaps hypothetical, privacy concerns that were clearly not anticipated at

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
		on websites, or who contribute to newsgroup discussions (Bennett, 2001, p.201).	based on a crude logic of probability (Bennett, 2001, p.201).	the time of the product development (Bennett, 2001, p.200).
		Spammers are free-riders. The real expense of their work is passed onto ISPs who suffer under the strain of processing junk e-mail through overburdened servers and committing time to dealing with subscriber complaints (Bennett, 2001, p.201).	There is general agreement that spam is a nuisance, that requires strong technical and perhaps legal defences (18 as cited by Bennett, 2001, p.201).	We can detect a steady and deliberate attempt to peel away the mask of anonymity provided by the original design of the Internet in order to discover who is browsing where, for what, and for how long (Bennett, 2001, p.201).
		A more sophisticated form of surveillance by design is revealed through the emerging practice of banner-advertising. The company whose practices have attracted the most media and political attention is Doubleclick, the top advertising company on the web (19 as cited by Bennett, 2001, p.201).	Any website that knows your identity and has a cookie for you could set up procedures to exchange their data with the companies that buy advertising space from them, synchronizing the cookies they both have on your computer (Bennett, 2001, p.202).	The initial manifestation of online surveillance is captured by the practice of spam e-mailing (Bennett, 2001, p.201).

Patterns of surveillance – Lit Review

Online v Offline	1970 v 1990	Surveillance Practices	Monitor v Monitored	Anonymity
		There is evidence, however, that cookie technology might be tracking device of the past (Bennett, 2001, p.202).	Among the information collected is the IP address of the computer that the Web Bug is sent to, the URL of the page of the Web Bug comes from and time it was viewed (25 as cited by Bennett, 2001, p.202).	This possibly means that once your identity becomes known to a single company listed on your cookies file, any of the others might know who you are every time you visit their sites (Bennett, 2001, p.202).
		In the summer of 2000, the phenomenon of the "Web Bug" entered the lexicon of the privacy advocacy community (Bennett, 2001, p.202).		This identity might become known by filling in a warranty, product registration, survey or purchase form (Bennett, 2001, p.202).
		According to the Privacy Foundation a Web Bug is a "graphic on a Web page or in an email message that is designed to monitor who is reading the Web page or email message. A Web Bug is often invisible because they are typically only 1-by-1 pixel in size, with no color (Bennett, 2001, p.202).		