David Lyon

Das Ende der Privatsphäre?

Seit Ende des zwanzigsten Jahrhunderts provoziert die inflationäre Verbreitung von Überwachungssystemen in der nördlichen Hemisphäre immer wieder die Frage, ob diese Entwicklung das „Ende der Privatsphäre" einläutet. Wie ist dieser Ausdruck zu verstehen? Einerseits gibt es, wie viele sozialkritische Autoren anmerken, immer weniger „Verstecke" (vgl. etwa O'Harrow 2005), da manche Überwachungssysteme so viele unserer tagtäglichen Aktivitäten und Routinen aufzeichnen, überwachen und verfolgen, dass scheinbar nichts, was wir tun, unbeobachtet bleibt. Andererseits beschreibt eine andere Gruppe von Autoren das „Ende der Privatsphäre" als eine Entwicklung, die regelrecht Anlass zum Jubeln oder doch zumindest keinen Anlass zur Sorge gibt. Angesichts der Verbreitung von E-Commerce und der damit verbundenen Weitergabe persönlicher Daten tätigte Scott McNealy von Sun Microsystems die viel zitierte Aussage: „Es gibt keine Privatsphäre mehr. Vergessen Sie es!"

Es scheint wichtig anzumerken, dass Privatsphäre ein überaus wandelbarer, sowohl historisch als auch kulturell relativer Begriff ist. Wenn betont wird, dass es keine Privatsphäre mehr gibt, dann bezieht sich dies auf eine Form der Privatsphäre, die eine relativ neue Erfindung der westlichen Welt ist (juristisch gesehen auf das persönliche Eigentum und besonders die Person als Eigentum bezogen). Gleichzeitig existiert diese westliche Vorstellung von Privatsphäre in manchen Ländern Südostasiens oder des Ostens schlichtweg nicht. Menschen in China haben eine andere Vorstellung von persönlichem Raum als Menschen aus dem Westen, und im Japanischen gibt es kein Wort für Privatsphäre (das Wort, das Japaner für „Privatsphäre" verwenden, wurde aus dem Westen entlehnt).

Der bekannteste Autor, der sich mit Privatsphäre im Computerzeitalter beschäftigt, ist Alan Westin, dessen Klassiker *Privacy and Freedom* (Westin 1967) zahlreiche Analytiker und politische Entscheidungsträger auf der ganzen Welt inspiriert und beeinflusst hat. Für ihn bedeutet Privatsphäre, dass „...Individuen, Gruppen oder Institutionen das Recht haben, Informationen über sich selbst zu kontrollieren, zu bearbeiten, zu verwalten und zu löschen sowie zu entscheiden, wann, wie und in welchem Umfang sie an andere weitergegeben werden". Auch wenn sich diese Definition nicht nur auf das „Individuum" zu beziehen scheint, so liegt doch die Verantwortung dafür, etwas gegen die ungerechtfertigte Nutzung persönlicher (und anderer Daten) „zu tun", bei den Datensubjekten. Anstatt sich auf die Verantwortlichkeit derer zu konzentrieren, die derartige Daten archivieren, wird einfach jenen, die Beschwerden haben, das Recht zugestanden, dass auf diese eingegangen werden muss.

Diese Akzentverschiebung wurde beispielsweise von Priscilla Regan (1995) kritisiert, die argumentiert, dass Privatsphäre einen intrinsischen, allgemein bedeutsamen, öffentlichen und sozialen Wert verkörpert und der Einzelne deshalb nicht nur das Recht hat, Schutz vor den Folgen einer missbräuchlichen Nutzung persönlicher Daten zu verlangen, sondern dass Institutionen, die auf derartige Daten zugreifen, vielmehr die Pflicht haben, Rechenschaft über die Nutzung von Daten abzulegen. Die umfassende Verbreitung von Überwachungstechnologien, etwa am Arbeitsplatz oder in der Exekutive, macht diese Forderung noch einsichtiger. Daten werden heute nicht nur archiviert und abgefragt, sondern auf eine Art und Weise analysiert, durchsucht, ausgewertet, neu kombiniert und innerhalb von bzw. zwischen Organisationen weitergegeben, die eine simple Definition von Privatsphäre schlicht unzulänglich erscheinen lässt. Während Westin in den 1960er Jahren mit einer breiter gefassten Definition von Privatsphäre operierte, hat das vorwiegend individualistisch geprägte Umfeld US-amerikanischer Geschäfts- und Regierungsinteressen und der Druck zur Berücksichtigung neuer technischer „Lösungen" laut Valerie Steeves

dazu beigetragen, den Begriff der Privatsphäre auf die aktuelle sehr knappe Definition einzuengen (Steeves 2005).

Überwachung als soziale Klassifikation

Zu behaupten, dass die Privatsphäre der modernen Überwachungstechnologie vielleicht nicht in all ihren Facetten zu widerstehen vermag, ist eine Sache. Etwas anderes ist es, eine geeignete Alternative vorzuschlagen. Denn wie die Orwell'sche und panoptische Metaphorik, derer man sich häufig bedient, um aufzuzeigen, was Überwachung bedeutet, genießt die Rede von der Privatsphäre breites Ansehen. Es ist schwierig Argumente dafür zu finden, warum die Verletzung der „Privatsphäre" nicht das (einzige) Problem ist, das Überwachung mit sich bringt (Stalder 2002), wenn dies von Rechtsanwälten, Politikern, Massenmedien und der westlichen Öffentlichkeit allgemein angenommen wird. Die beste Möglichkeit, die Aufmerksamkeit von einer ausschließlichen Fokussierung auf die Privatsphäre abzuwenden, ist meiner Meinung nach, Überwachung als „soziale Klassifikation" zu sehen.

Man könnte sagen, dass „Klassifizieren menschlich ist"; in Zeiten der Moderne hat der Prozess der Klassifikation sich jedoch zu einer wahren Industrie entwickelt. Von der Medizin bis zum Militär ist Klassifikation unerlässlich. Wie Geoffery Bowker und Susan Star aufzeigen, schafft die Suche nach verwertbarem Content den Wunsch nach Klassifikation und das Bestreben, „Dinge zu ordnen" (Bowker und Star 1999). Jede Form von Klassifikation basiert auf menschlichen Urteilen und das ist aus unserer Sicht entscheidend. Durch Klassifikation kann man unerwünschte Elemente aussondern (etwa solche, die anfällig für bestimmte Krankheiten sind); dieser Mechanismus kann jedoch leicht in negative Diskriminierung umschlagen. Südafrika hatte zu Zeiten der Apartheid ein umfassendes System zur Klassifikation seiner Bevölkerung, das jedoch dazu verwendet wurde, Menschen mit schwarzer Hautfarbe aufgrund ihrer „Rasse" vom gleichberechtigten Zugang zu Ressourcen auszuschließen. Klassifikation kann harmlos und für die Menschheit nützlich sein, sie kann jedoch ebenso gut die Grundlage für Ungerechtigkeit und Ungleichheit darstellen. Der moderne Klassifikationsdrang fand im Computer sein ideales Instrument.

Betrachtet man Überwachung als soziale Klassifikation, sollte man sich in Erinnerung rufen, dass die heutigen Überwachungssysteme stark auf IKT-Anwendungen basieren. Sowohl Sicherheitssysteme als auch Marketingtechniken nutzen die Interaktivität von IK-Technologien, um für die jeweilige Institution interessante Zielgruppen und Individuen zu identifizieren und isolieren. Durch die Speicherung von Daten über Menschen und deren Aktivitäten und Bewegungen sowie die Analyse von Sekundärdaten (beim Durchsuchen anderer Datenbanken gewonnener Daten) mittels vernetzter Technologien können Marketingexperten ihre Werbe- und Marketingkampagnen mit größerer Exaktheit planen und auf ihre Zielgruppen ausrichten. Ähnliche Strategien nutzen auch Sicherheitsexperten, um bereits früher identifizierte oder einem bestimmten Profil entsprechende „Verdächtige" zu überwachen, in der Hoffung, besseren Einblick in das Leben dieser Personen zu gewinnen, alle ihre Bewegungen verfolgen und so Gewalt- oder Terrorakte verhindern zu können.

Dieser versicherungsmathematische Zugang zur Chancenmaximierung (Marketingstrategien zur besseren Erschließung der Zielgruppen für Produkte und Dienstleistungen) bzw. Risikominimierung (Sicherheitsmaßnahmen zur besseren Überwachung verdächtiger Gruppen) stellt eine neue Entwicklung im Bereich der Überwachung dar. Obwohl derartige Ansätze auf eine lange Geschichte zurückblicken können, unterscheiden sie sich doch von konventionelleren reaktiven Marketing- oder Überwachungsmethoden. Sie sind stärker zukunfts- und weniger vergangen-

heitsorientiert und basieren auf der Simulation und modellhaften Darstellung von Situationen, die erst eintreten müssen. Sie können nicht ohne vernetzte, abfragbare Datenbanken operieren; die Neuheit dieses Zugangs zeigt sich etwa darin, dass ahnungslose Bürger, die beispielsweise einem bestimmten Altersprofil entsprechen, E-Mails erhalten, in denen ihnen Mittel zur Potenzsteigerung angeboten werden, und andere, was weit weniger amüsant ist, einfach nur weil sie einem bestimmten ethnischen oder religiösen Profil entsprechen, überwacht und ohne Angaben von Gründen oder sogar von Sicherheitskräften festgehalten werden können.
Die „Überwachungsmaschinerie" operiert mit sozialer Klassifikation. Verschiedene abstrakte Daten (Videos, Textdateien, biometrische Daten, genetische Information, etc.) werden manipuliert, um in einem sich stetig verändernden Netzwerk Profile und Risikokategorien erstellen zu können. Planung, Vorhersage, Vorrechte und Genehmigungen – um diese und andere Ziele geht es, wenn die Maschinerie anrollt und für die eigenen Zwecke genutzt wird. Soziale Klassifikation ist einerseits ein uraltes, vielleicht zutiefst menschliches Verhalten; heute jedoch ist der Klassifikationsvorgang zur Routine geworden; er wurde systematisiert und vor allem technisiert und automatisiert (wenn nicht gar regelrecht von der Technik getrieben). Je mehr neue Technologien involviert sind, desto undurchsichtiger werden die Klassifikationskriterien für die Öffentlichkeit. Wer weiß, auf welcher Grundlage ein Kreditantrag unerwartet abgelehnt oder ein unschuldiger Terrorismusverdächtigter festgehalten wurde? Natürlich kann der Auswahlprozess harmlos und gerechtfertigt sein – Überwachung ist schließlich immer eine zweischneidige Angelegenheit; soziale Klassifikation hat jedoch auch immer direkte Folgen (zum Guten oder Schlechten) für die Lebenswirklichkeit von Menschen (für Beispiele vgl. Lace 2005:28–32).
Zu den größten Ängsten, die mit einer Automatisierung der sozialen Klassifikation verbunden sind, zählt daher für viele, dass große Organisationen mittels relativ unberechenbarer Mechanismen Urteile fällen, die direkten Einfluss auf das Leben derer nehmen, deren Daten von den Organisationen verarbeitet werden. Im Geschäftsbereich werden derartige Entscheidungen nach versicherungsmathematischen Kriterien getroffen und basieren meist auf Risikobewertungen; als bestes Beispiel können hier die im Zusammenhang mit Versicherungsverträgen angestellten Risikoeinschätzungen genannt werden. Antragsteller werden vielleicht aufgrund ihres Wohnorts und anderer soziodemografischer Faktoren klassifiziert und zur Zahlung von Versicherungsprämien angehalten, die nur in geringem Zusammenhang mit anderen grundlegenden Faktoren stehen. Ebenso werden Konsumenten zunehmend nach bestimmten für ein Unternehmen interessanten Kategorien klassifiziert, aus denen sie entweder Vorteile für sich ziehen oder von der Teilnahme am Marktgeschehen ausgeschlossen werden können. Im Bereich der Exekutive wird dieser versicherungstechnische Ansatz weiter repliziert; so warnten beispielsweise Feely und Simon Mitte der 1990er Jahre davor, dass sich allmählich Formen einer „versicherungsmathematischen Gerechtigkeit" abzeichnen. Die „neue Pönologie", so argumentieren sie, „beschränkt sich auf Techniken zur Identifikation, Verwaltung und Klassifikation von Risikogruppen nach verschiedenen Gefährlichkeitsgraden" (Feely and Simon 1994:180). Anstatt kriminelles Verhalten aufgrund von Beweisen zu belegen, konzentriert man sich im Rahmen derartiger neuer Ansätze auf präventive Intervention auf der Basis von Risikoanalysen – ein Trend, der sich nach 9/11 weiter verstärkt hat.

Überwachungsgesellschaft und Sicherheitsstaat

Der Ausbau des Überwachungsapparats moderner Staaten verdient besondere Beachtung, und eine der Möglichkeiten, darauf hinzuweisen, ist die Beschreibung unserer heutigen Lebenswirklichkeit als „Überwachungsgesellschaft". Damit soll kein düsteres, Unheil verkün-

dendes Szenario heraufbeschworen werden, sondern schlicht zum Ausdruck gebracht werden, dass beispielsweise auch die Speicherung persönlicher Daten im Supermarkt eine Form der „Überwachung" ist. Der Ausdruck „Überwachung" lenkt unsere Aufmerksamkeit auf ein zentrales Phänomen unseres täglichen Lebens, das so allgegenwärtig und selbstverständlich geworden ist, dass es gar nicht weiter auffällt, auch wenn es derart weit reichende Konsequenzen hat, dass es von der Sozialwissenschaft auf das Genaueste untersucht werden sollte.

Gleichzeitig spiegelt das Leben in einer Überwachungsgesellschaft teilweise eine neue Dimension des Nationalstaates. Während es Mitte und Ende des zwanzigsten Jahrhunderts vielleicht richtig war, wenn sich einige liberalere Länder als „Wohlfahrtsstaat" betrachteten, so war der Ausdruck „Sicherheitsstaat" für die Situation zu Beginn des zwanzigsten Jahrhunderts ein weitaus plausiblerer Deskriptor (Raab 2005). Bei der Bewertung verschiedener Maßnahmen steht immer öfter nicht der Nutzen dieser Maßnahmen für die Allgemeinheit im Vordergrund, sondern vielmehr das Kriterium der Risikominimierung. Neue Technologien zur Risikominimierung sind ein zentrales Merkmal für das sich abzeichnende Streben nach einem „Sicherheitsstaat"; und alle diese Technologien gehen mit irgendeiner Form der Überwachung einher.

In ihren Studien zur Polizeiarbeit zeigen Ericson und Haggerty auf, wie neue Kommunikationstechnologien eine schnellere Übertragung möglich machen und zu einem Wechsel von lokalen, räumlichen Zentren hin zu „Mikrozentren der Inskription" wie z. B. Computerterminals in Polizeiautos beitragen (1997:431). Von den gleichen Trends werden Organisationshierarchien in Frage gestellt, gleichzeitig wird aber auch die „Fernkontrolle" erleichtert. Gemeinsam ermöglichen diese neuen Technologien eine schnellere Überwachung der Bevölkerung zum Zweck des Risikomanagements (während gleichzeitig auch die Polizei anfälliger für Kontrolle wird). Was Ericson und Haggerty über die Polizeiarbeit sagen, zeichnet sich auch in anderen Bereichen ab. Überwachung ist grundlegend für die Risikominierung, weil sie „Kriterien für die Festlegung von Grenzwerten liefert, die dazu dienen, annehmbare Risiken zu definieren und die Einbindung bzw. Ausgrenzung von Akteuren zu rechtfertigen". Dadurch, so Ericson und Haggerty, „weichen Kontrolle und Zwang einer kontingenten Kategorisierung" und jeder „gilt als ‚schuldig', solange das Überwachungssystem keine gegenteiligen Informationen liefert ..." (1997:449).

Seit 9/11 haben sich derartige Entwicklungen im Westen weiter verbreitet und sind fragwürdiger geworden. Die Warnstufen von Flughafen- und Grenzsicherheitssystemen werden nach diesen Kriterien hinaufgesetzt. Die gleichen Überwachungssysteme, inzwischen weiter verstärkt durch den Einsatz von „neuen" biometrischen Technologien (diese unterscheiden sich von den „alten" nicht etwa, weil sie ihren oft rassistischen und kolonial geprägten „anthropometrischen" Ursprung hinter sich gelassen hätten, sondern wegen ihrer umfassenden Nutzung von IKTs), werden eingesetzt, um „biografische" Profile ganzer Bevölkerungsgruppen zu erstellen und zu entscheiden, ob Angehörige dieser Gruppen reisen, große Geldbeträge überweisen oder bei bestimmten Unternehmen beschäftigt werden dürfen oder nicht. Daher sorgte auch der Einsatz von „Schwarzen Listen für unerwünschte Flugpassagiere", die aufgrund der ethnischen Abstammung, Religion oder Herkunft der inkriminierten Passagiere erstellt werden, unter Bürgerrechtlern für einen Skandal – nichts leichter, als aufgrund von „Verwechslungen" auf eine derartige Liste zu geraten. Und daher auch die ironische Verschärfung des Risikos (für Reisende und Bürger) durch die vermehrte Auslagerung von derartigen Aufgaben auf andere Einrichtungen (etwa Flughäfen), besonders in Ländern wie den USA.

Wegen der Rolle der IKTs ist es unter anderem auch wichtig, „Überwachungsgesellschaft" und „Sicherheitsstaat" gemeinsam zu betrachten. Denn die Risikokommunikation (als Synonym könnte hier auch „Chancenbewertung" stehen), die Unternehmen in Bezug auf ihre Kunden

betreiben, und die Erstellung von detaillierten Profilen sind auch für den Nationalstaat von Interesse. Nicht nur basiert die Profilerstellung auf ähnlichen Algorithmen, sondern auch die von diesen Unternehmen archivierten und analysierten Daten selbst sind für die Exekutive von Interesse, besonders im so genannten „Krieg gegen den Terrorismus". 2006 weigerte Google sich beispielsweise, seine Protokolle über Suchanfragen der Benutzer an das US-Justizministerium auszuhändigen, indem man sich auf die Wahrung der Privatsphäre der Benutzer und den Schutz des Geschäftsgeheimnisses berief. Die Begründung des Ministeriums lautete, dass man die Wirksamkeit einer Web-Filtering-Software testen wollte, viele Bürgerrechtler und Datenschützer sahen in dieser Forderung jedoch einen ersten Versuch, sich Zugriff auf bestimmte Daten zu verschaffen. Die Regierung könnte derartige Protokolle auch nutzen, um im Namen der „nationalen Sicherheit" Zugang zu höchst sensiblen persönlichen Daten zu erlangen.
Während es durchaus sinnvoll erscheint, die Entwicklung der „Überwachungsgesellschaft" (in Bezug auf ihre zum Standard gewordene Abhängigkeit von der Speicherung und Verarbeitung persönlicher Daten) und des „Sicherheitsstaats" (in Bezug auf seine Nutzung von Überwachungssystemen für die Risikobeurteilung) einzeln zu analysieren, ist es auch wichtig, aufzuzeigen, dass die beiden in einer zunehmend symbiotischen Beziehung zueinander stehen. Wenn die gegenwärtige Entwicklung andauert, wird diese spezifische sozioökonomisch-politische Verkettung in den kommenden Jahrzehnten immer wichtiger werden.

Politik der persönlichen Daten

Die *Surveillance Studies,* wie die Subdisziplin, die sich mit Überwachung und den damit verknüpften Phänomenen beschäftigt, vermehrt genannt wird (vgl. Lyon, im Druck), haben sich häufig auf die großen Systeme, Institutionen und Technologien konzentriert, die Überwachung forcieren und ermöglichen. Diese Schwerpunktsetzung kann allerdings zu einer negativen und dystopischen Perspektive führen, die den Eindruck erweckt, dass gewöhnliche Menschen, deren alltägliche Aktivitäten überwacht werden, einfach nur Bauern in einem Schachspiel, Chiffren in einem zunehmend global agierenden Überwachungsapparat sind. Zweifelsohne ist eine derartige Sichtweise berechtigt, und es steht fest, dass das Mächtegleichgewicht von den großen Institutionen bestimmt wird; dennoch ist es wichtig anzumerken, dass Überwachung ein interaktiver Prozess ist. Der von Techniksoziologen gerne gebrauchte Begriff der „Ko-Konstruktion" beschreibt die Welt der Überwachung sehr gut (Lyon, 2004).
Um funktionieren zu können, sind Überwachungssysteme von ihren Subjekten abhängig (die Subjekte werden, wie Foucault bereits vor langer Zeit anmerkte, sogar zu „Trägern der eigenen Überwachung", 1977). Obwohl die Subjekte der Überwachung in gewissem Sinn „objektiviert" werden, wenn ihre Datendoppelgänger für das Überwachungssystem realer werden als ihr Körper und das tägliche Leben, auf dem diese Daten basieren, erfolgt ihre Interaktion mit dem Überwachungssystem oft aktiv, bewusst und intentional. Menschen erfüllen die Regeln der Überwachungssysteme (sie werden keineswegs übertölpelt), sie verhandeln mit den Systemen, in die ihr Leben verstrickt ist, und widersetzten sich diesen bisweilen.
Es scheint sehr wichtig, näher darauf einzugehen, wie die so genannten „Datensubjekte" der Überwachungssysteme mit diesen interagieren und wie sie damit umgehen, dass ihre Daten von Organisationen archiviert und genutzt werden. Der Zweck, zu dem die Daten gespeichert werden, ist wesentlich. Ein Flugpassagier mit einem „verdächtigen" Namen ist vielleicht zutiefst empört darüber, dass er von einem Flug ausgeschlossen wird, wird sich aber vermutlich durchaus erfreut über „Vorteile" zeigen, die er aufgrund des Vielfliegerprogramms genießt, über das er

sein Flugticket „gekauft" hat. In beiden Fällen kommt das Ergebnis aufgrund der Nutzung einer Vielzahl persönlicher Daten zustande, egal ob es in die Kategorie „privilegierter Elitepassagier" oder „Name auf einer schwarzen Liste" fällt. Konsumenten geben ihre persönlichen Daten oft allzu bereitwillig bekannt, im Glauben, dass sie davon profitieren; wogegen Angestellte und Bürger mit ihren Daten meist weitaus vorsichtiger umgehen und ihrem Unbehagen über das übereifrige Bemühen von Institutionen um ihre persönlichen Daten eher Ausdruck verleihen.
Bei der Analyse der Interaktionen zwischen „Beobachtern und Beobachteten" spielt auch eine Rolle, ob die „Datensubjekte" wissen, dass sie beobachtet werden. Im klassischen Fall der panoptischen Überwachung wurde von Gefängnisinsassen Selbstdisziplin erwartet, da der unsichtbare Aufseher sie ja gerade beobachten könnte. Unsicherheit ist wesentlich für das System. Wie gehen wir jedoch mit Situationen um, in denen die Kameras versteckt sind, oder in denen Kundeninformationen einfach ohne das Wissen der betroffenen Person abgefragt werden? Auch in diesen Fällen werden die Lebensrealität und Wahlmöglichkeiten der Menschen (zum Guten oder Schlechten) beeinflusst, ihre Möglichkeiten zur Interaktion mit dem Überwachungssystem sind jedoch stark eingeschränkt. Je häufiger IKTs dazu beitragen, die Sichtbarkeit von Überwachungsmechanismen durch die Miniaturisierung oder Automatisierung dieser Mechanismen zu reduzieren, desto wichtiger wird diese Frage für weitere soziale und politische Analysen werden.
Die Beweislage deutet darauf hin, dass die Bedeutung der Informationspolitik weiter zunehmen wird, auch wenn mancher führende Informationstheoretiker dies anders sieht. Manuel Castells versichert seinen Lesern beispielsweise, dass moderne Überwachungssysteme meistens eher harmlose Routinen umfassen, und Scott Lash argumentiert, dass mit der „Dominanz der Kommunikation die Logik der Klassifikation verschwindet" (2002:112). Ich habe versucht in diesem Beitrag aufzuzeigen, dass die Nutzung von IKTs im Rahmen neuer Ausprägungen des Risikomanagements in der Überwachungsgesellschaft und im Sicherheitsstaat zu neuen Formen der Klassifikation führt, die tief greifende soziale, ökonomische und politische Veränderungen mit sich bringen. Dies ist die Arena, in der der Kampf um Information ausgetragen werden wird.

Bei diesem Text handelt es sich um einen Auszug aus einem Beitrag von David Lyon im *The Oxford Handbook of Information and Communication Technologies,* herausgegeben von Robin Mansell, Chrisanthi Avgerou, Danny Quah und Roger Silverstone, © Oxford University Press, 2007; abgedruckt mit freundlicher Genehmigung des Verlags.
Für weitere Informationen: http://www.oup.com/uk/catalogue/?ci=9780199266234.

Aus dem Englischen von Sonja Pöllabauer

O'Harrow R. (2005), *No Place to Hide,* New York: Free Press.
Westin, A. (1967), *Privacy and Freedom,* New York: Athenaeum.
Steeves, V. 2005 "It's not child's play: The online invasion of children's privacy," *University of Ottawa Law and Technology Journal,* 2 (2).
Stalder, F. (2002), "Privacy is not the antidote to surveillance", *Surveillance and Society* 1(1)
Bowker, G. and Star, Susan. (1999), *Sorting things out: Classification and its consequences,* Cambridge MA: MIT Press.
Lace, S. (2005) The Glass Consumer: *Life in a Surveillance Society,* Bristol UK: The Policy Press
Feely M.and Simon, J. (1994) "Actuarial justice: the emerging new criminal law" in D.Nelken ed. *The Futures of Criminology,* London: Sage.
Raab, C. D. (2005), "Governing the safety state", inaugural lecture at the University of Edinburgh, Scotland (June 7).
Ericson, R. and Haggerty, K. (1997), *Policing the Risk Society,* Toronto: University of Toronto Press.
Lyon, D. (2004), "Surveillance technologies and surveillance societies", in T. Misa, P. Brey, and A. Feenberg, (eds.) *Modernity and Technology,* Cambridge MA: MIT Press.