Forschung

Preprint. Erscheint als: Friedewald, M. & Langheinrich, M. (2011). Datenschutzaspekte smarter Überwachung. *Digma – Zeitschrift Fuer Datenrecht Und Informationssicherheit*, *11*(3), 118–120.

Datenschutzaspekte smarter Überwachung

Dr. Michael Friedewald
Koordinator Forschungsgruppe „Informations- und Kommunikationstechnik", Fraunhofer-Institut für System- und Innovationsforschung, Karlsruhe, Deutschland, michael.friedewald@isi. fraunhofer.de

Prof. Dr. Marc Langheinrich
Università della Svizzera italiana (USI), Lugano, langheinrich@acm.org

Moderne „intelligente" Überwachungssysteme sollen den Bürger besser vor Terrorismus und organisierter Kriminalität schützen, greifen potentiell aber tief in die Privatsphäre des Einzelnen ein. Das EU-Forschungsprojekt SAPIENT untersucht die Risiken solcher intelligenten Überwachungstechniken und erarbeitet Verfahren, um diese im Einklang mit Menschenrechten und unter Beachung des sozialen und gemeinschaftlichen Zusammenhalts gestalten zu können.

Als Folge der Terrorangriffe vom 11. September 2001 ist Überwachungstechnik von Politik und Industrie zu einem wichtigen Mittel zur Wahrung der öffentlichen Sicherheit erklärt worden. Neue, „intelligente" Überwachungstechniken (sowie Kombinationen oder Assemblagen solcher Techniken) sollen vordergründig zum Kampf gegen Terrorismus, organisierte Kriminalität und illegale Einwanderung verwendet werden, können aber auch für eine Vielzahl anderer Zwecke genutzt werden, die in die Privatsphäre gesetzestreuer Bürger eingreifen und so erhebliche Risiken für die bürgerlichen Grundrechte bergen.[i]

Neue Herausforderungen

Intelligente Überwachung

Während der Begriff „Überwachungstechnik" im ausgehenden 20. Jahrhundert noch hauptsächlich mit einfachen Videoüberwachungs- und Telefonabhöranlagen in Verbindung gebracht wurde, reichen moderne Überwachungssysteme längst über einfache Audio- und Videoübertragung hinaus. Neue Sensoren ermöglichen die Erfassung sowohl kleinster physiologischer Symptome (z.B. mittels lasergestützter Temperaturfernmessung) als auch flächendeckender Merkmale (z.B. den aktuellen Verkehrsfluss durch Analyse der Bewegungsmuster von Mobiltelefonen). Leistungsstarke Computernetze erlauben die einfache und effektive Verbreitung solcher Daten an praktisch jeden Ort der Welt, in beinahe Echtzeit. Die zunehmende Miniaturisierung von Computern ermöglicht darüber hinaus die Integration von komplexen Vorverarbeitungsschritten (DSP, digitale Signalverarbeitung) direkt auf Kamera oder Mikrofon (z.B. Bewegungserkennung und Geräuschunterdrückung) während

zentrale Serveranlagen die Analyse und Koordination einer praktisch unbegrenzten Anzahl solcher (digitalen) Signale erlauben. Und schlussendlich unterstützen moderne Datenbanken komplexe automatisierte Abfragen, die immense Datenmengen kontinuierlich nach Mustern und Anomalien absuchen können bzw. verstreute Informationen virtuell zu detaillierten Dossiers zu verknüpfen vermögen.

Clarke (1988) prägte bereits früh den Begriff „Dataveillance“ für diese auf digitalen Informationen beruhende Universalüberwachung. Wright et al. (2010) bezeichnen die Kombination aus Datenintegration, algorithmischer Analyse und neuen Sensorsystemen als „intelligente Überwachung“ (smart surveillance). Intelligente Überwachungssysteme können gezielt anwendungsspezifische Informationen aus einer grossen Anzahl Datenströmen extrahieren, diese in spezifische Ereignisbeschreibungen übersetzen und so voll- und halbautomatische Entscheidungsprozesse unterstützen.

Die Banalisierung der Überwachung

In einigen EU-Ländern (z.B. in Großbritannien) ist moderne Überwachungstechnik schon heute allgegenwärtig. Dabei ist ihr Einsatz schon lange nicht mehr auf die Strafverfolgungsbehörden, Geheimdienste und das Militär beschränkt: So werden bereits heute der Verkehr auf den Straßen, Passagiere auf Bahnhöfen und Flughäfen überwacht; staatliche Stellen überprüfen mit intelligenten Systemen ob Antragsteller berechtigt sind, Sozialleistungen in Anspruch zu nehmen; Unternehmen überwachen E-Mail-Kommunikation, besuchte Websites oder sogar Tastenanschläge ihrer Mitarbeiter; Internet-Service-Provider überwachen den Datenverkehr, um ihren Kunden personalisierte Werbung präsentieren zu können.

Überwachung ist also schon seit einiger Zeit nicht mehr auf den Bereich der inneren Sicherheit beschränkt, sondern dringt allmählich und vielfach unbemerkt immer tiefer in unser tägliches Leben ein.

Diese Veralltäglichung oder Banalisierung wird auch dadurch befördert, dass viele Anwendungen in diesem Bereich längst nicht mehr einen repressiven Charakter zur Schau stellen, sondern sich als eine Vielzahl von nützlichen Helfern präsentieren. Überwachung wird so mehr und mehr zu einem normalen Element der sozialen, politischen und ökonomischen Beziehungen.

Man denke hier beispielsweise an den zunehmenden Einsatz von Videoüberwachung im privaten Bereich, RFID-basierte Schliess- und Bezahlsysteme (die sogenannten „kleinen Schwestern“ des „großen Bruders“[ii]) oder die Nutzung biometrischer Identifikationssyteme selbst für banale Anlässen. Ein Beispiel aus dem Bereich der Strafverfolgung ist der mittlerweile massenhafte Einsatz von DNA-Tests selbst bei geringfügigen Straftaten.[iii]

In vielen Fällen mögen Bürger die zunehmende Überwachung als etwas akzeptieren, das sie nicht ändern können und was ansonsten kontinuierlich unangenehme Gefühle hervorrufen würde. Die Banalisierung führt jedoch auch Schritt um Schritt zu einer graduellen, schließlich aber doch signifikanten Verschiebung der Maßstäbe für die Verhältnismäßigkeit von Überwachung, mit potentiell weitreichenden Folgen für die gesellschaftliche Debatte in diesem Bereich.

Überwachung und europäische Innen- und Sicherheitspolitik

Die Europäische Union hat bereits seit längerem das problematische Potential von intelligenten Überwachungstechnik erkannt. Die EU Kommission fordert beispielsweise in ihrem Stockholmer Programm, es müsse eine „Ausgewogenheit zwischen Überwachung und Kontrolle zur Minimierung möglicher Auswirkungen von terroristischen Maßnahmen und der Beachtung der Menschenrechte, der Privatsphäre, des sozialen und gemeinschaftlichen Zusammenhalts sowie die erfolgreiche Integration von Minderheitsgemeinschaften ... hergestellt werden“.[iv]

Dementsprechend werden im EU-Forschungsrahmenprogramm auch wissenschaftliche Untersuchungen gefördert, die sich mit der Frage auseinandersetzen, welche Risiken mit intelligenten Überwachungstechniken verbunden sind und wie man die geforderte Ausgewogenheit herstellen kann. Dies ist Gegenstand des Projekts SAPIENT (Supporting fundamental rights, privacy and ethics in surveillance technologies), welches im Folgenden kurz beschrieben werden soll.

Das Projekt SAPIENT

Ziele und Forschungsfragen

Ein erstes Projektziel besteht darin zu analysieren, wie und wann intelligente Überwachungstechnik eingesetzt werden sollte (oder auch nicht) und welche Eigenschaften für eine effektive Nutzung in sich schnell ändernden Umgebungen entscheidend sind. Davon ausgehend soll unter Berücksichtigung anerkannter Datenschutzprinzipien ein Kriterienkatalog entwickelt werden, der Entscheidungsträger (in Politik, Behörden und Unternehmen) in die Lage versetzen kann, frühzeitig (möglichst a priori) abzuschätzen, ob eine bestimmte Überwachungstechnik oder deren Anwendungen das Recht der Bürger auf Privatsphäre gefährdet.

Zu diesem Zweck entwickelt das Projektteam eine Methode zur Datenschutzbewertung (Privacy Impact Assessment, PIA), die auf intelligente Überwachungstechniken (insbesondere in Sicherheitsanwendungen) zugeschnitten ist. Dieses Instrumentarium sollte so verständlich und einfach zu nutzen sein, dass es sowohl von Entscheidungsträgern als auch von Technikentwicklern problemlos angewendet werden kann, um möglichst transparente, intervenierbare und nichtverkettbare Systeme[v] entwerfen zu können. Dazu wird sich das Projekt auf Fragen der Notwendigkeit und Verhältnismäßigkeit der Datenerfassung konzentrieren, um von vornherein Gefahren für die informationelle Selbstbestimmung und andere bürgerliche Grundrechte zu vermeiden. Nur so können Techniken und Praktiken der Überwachung entstehen, die die Achtung der Privatsphäre in den Mittelpunkt stellen und damit gesellschaftlich akzeptabel sind.

Vorgehensweise

In einem ersten Schritt definiert und charakterisiert das SAPIENT-Projekt Überwachungstechnik als seinen Untersuchungsgegenstand innerhalb des technischen, sozialen, politischen, rechtlichen und ethischen Kontexts, indem der Stand der verschiedenen Diskurse zusammengetragen und miteinander vergleichend analysiert wird. Dabei spielen vor allem

Wechselwirkungen und historische Entwicklungen in den vergangenen 10 Jahren eine bedeutende Rolle.

Im zweiten Schritt werden die Sichtweisen der Betroffenen mit den Sichtweisen der aktiv Handelnden aus staatlichen Einrichtung (Strafverfolgungsbehörden, Grenz- und Katastrophenschutz), Politik und Wissenschaft in Form von Fokusgruppen in den Forschungsprozess einbezogen. Diese sollen mögliche Szenarien der künftigen Überwachung diskutieren und bewerten. Auf diese Weise wird sichergestellt, dass alle relevanten Sichtweisen und Interessen in den zu erstellenden Kriterienkatalog für die Datenschutzbewertung einfließen.

Im dritten Projektschritt werden die heute existierenden Verfahren zur Datenschutzbewertung systematisch erfasst und analysiert. Besonderes Augenmerk liegt dabei bei solchen Verfahren, für die entweder bereits praktische Erfahrungen vorliegen (z.B. das PIA Handbuch des britischen Information Commissioner's Office[vi]) oder deren Einführung auf Ebene der Europäischen Union diskutiert wird (z.B. das EU-Rahmenwerk für die RFID-Datenschutzfolgeabschätzung[vii]). Auf Grundlage dieser Bestandsaufnahme und der im zweiten Arbeitsschritt ermittelten Anforderungen der Akteure und Betroffenen erarbeitet das Projektteam einen ersten Vorschlag für ein Rahmenwerk für die Datenschutzfolgeabschätzung von intelligenten Überwachungstechniken.

Im letzten Arbeitsschritt wird dieser Vorschlag durch eine Reihe von Konsultationen mit Datenschützern, Nichtregierungsorganisationen und Entscheidern diskutiert und anschließend an Hand ausgesuchter Fallstudien (u.a. biometrische Verfahren, intelligente Videoüberwachung) empirisch validiert. Die Ergebnisse dieser Fallstudien und die Erfahrungen bei deren Durchführung werden schließlich zur Verbesserung des Rahmenwerks genutzt.

Ein weiteres wichtiges Element des SAPIENT-Projektes ist die kontinuierliche Präsentation und Diskussion von Projektergebnissen mit allen relevanten Akteuren und die Herstellung von Transparenz gegenüber der Öffentlichkeit. Zu diesem Zweck werden regelmäßige Informationsveranstaltungen stattfinden. Am Ende des Projekts wird das Team zu einer Abschlußkonferenz einladen, auf der die Projektergebnisse nochmals erörtert und mögliche Ansätze zu deren Umsetzung eruiert werden sollen.

SAPIENT in Zahlen

Das Projekt SAPIENT (FP7- SEC-2010-1, GA 261698) ist ein EU-gefördertes Projekt im 7. Rahmenprogramm für Forschung und Entwicklung im Themenbereich «Sicherheitsforschung». Projektstart war der 1. Februar 2011 und innerhalb von drei Jahren wollen die sieben Projektpartner unter der Führung des Fraunhofer Instituts für System- und Innovationsforschung ihr ehrgeiziges Ziel erreichen. Zu den Partnern gehören das britische Beratungsunternehmen Trilateral Research & Consulting, das italienische Centre for Science, Society and Citizenship, das Centre for Law, Science and Technology Studies an der Vrije Universiteit Brussels, die Fakultät für Informatik an der Universität der italienischen Schweiz in Lugano, das Department of War Studies am King's College London sowie das Centre for European Policy Studies in Brüssel.

Literatur und weiterführende Links

- ROGER CLARKE, Information Technology and Dataveillance, Communications of the ACM, vol. 31, no. 5, May 1988, pp. 498-512.
- ROGER CLARKE, Privacy impact assessment: Its origins and development, Computer Law and Security Review, 25(2009), 123ff.
- SERGE GUTWIRTH, Privacy and the information age, Lanham 2002.
- DAVID WRIGHT/MICHAEL FRIEDEWALD/SERGE GUTWIRTH/MARC LANGHEINRICH ET AL., Sorting out smart surveillance, in: Computer Law and Security Review 26(2010), 343ff.
- DAVID WRIGHT/PAUL DE HERT (Hrsg.), Privacy Impact Assessment, Dordrecht 2012 (im Erscheinen).
- SAPIENT Website, Online: <http://www.sapient-project.eu>

---

[i] KEVIN D. HAGGERTY/RICHARD V. ERICSON, The surveillant assemblage, in: British Journal of Sociology 51(2000), S. 605ff.

[ii] VAN LIESHOUT, MARC/KOOL, LINDA, Little sisters are watching you: A privacy assessment of RFID, in: The Future of Identity in the Information Society (IFIP AICT 262), Berlin, Heidelberg 2008, 129-41.

[iii] MARX, GARY T., Soft Surveillance: The Growth of Mandatory Volunteerism in Collecting Personal Information, in: Monahan, T (Hrsg.), Surveillance and Security: Technological Politics and Power in Everyday Life, New York 2006, 37-56.

[iv] EUROPÄISCHE KOMMISSION, Ein Raum der Freiheit, der Sicherheit und des Rechts im Dienste der Bürger, KOM (2009) 262 endg.

[v] MARTIN ROST/ANDREAS PFITZMANN, Datenschutz-Schutzziele - revisited, in: DuD 6/2009, S. 353ff.

[vi] INFORMATION COMMISSIONER'S OFFICE, Privacy impact assessment handbook. Version 2.0, London 2009. http://www.ico.gov.uk/upload/documents/pia_handbook_html_v2/index.html (16.07.2011)

[vii] Privacy and Data Protection Impact Assessment Framework for RFID Applications, 12 January 2011, <http://cordis.europa.eu/fp7/ict/enet/documents/rfid-pia-framework-final.pdf> (16.07.2011)