klassische Abwehrrecht der Bürger vor staatlichen Eingriffen bleibt eine Aufgabe, ist aber heute nur noch die eine Seite der Medaille.

Will sich der Gesetzgeber gegenüber Google & Co Geltung verschaffen, kann er nicht wie im alten System des Datenschutzes von isolierten Datensätzen mit Einzelangaben wie Name, Familienstand und Wohnungsgröße denken. Apps, Suchmaschinen und soziale Netzwerke sind viel komplexer und verlangen andere Regelungstechniken.

Der Schutz vor digitaler Diskriminierung, Identitätsmissbrauch, unbefugtem Zugriff auf eigene IT-Systeme, Ehrverletzung und finanziellen Schäden kann nicht mehr durch einen Eingriff in die Vielfalt der freien Internetdienste oder die gesetzliche Beschreibung von Datenverarbeitungsvorgängen gewährleistet werden. Das Bundesverfassungsgericht betont in seiner Rechtsprechung die zentrale Bedeutung des Persönlichkeitsschutzes als Aufgabe und Ziel. Es hat mit seinem IT-Grundrecht in eine Richtung gewiesen, die wir auch in Europa für zukunftsweisend halten. Dazu gehört auch die Definition von Verantwortlichkeiten. Nehmen wir das Thema „Cloud-Computing". Wer ist hier eigentlich für was verantwortlich?

Fazit: Wir müssen daran arbeiten, die EU-Datenschutzverordnung moderner und innovativer zu gestalten, um sie passend für eine vernetzte Informationsgesellschaft zu machen. Der Freiheitsgewinn von Google, Facebook, Twitter & Co darf dabei nicht außer Acht gelassen werden. Die faktische Abschaffung all dieser Dienste wäre kein grundrechtliches Paradies. Es ginge auch gar nicht.

Auf die digitale Vernetzung können wir nicht nur europäische Antworten geben. Parallel zum Europäischen Datenschutztag wird in den USA und Kanada der „Data Privacy Day" begangen. Die Yottabyte an Daten, die uns heute im Internet umgeben und die wir selbst täglich vermehren und nutzen, werden international erhoben und verarbeitet. Wir sind auf internationale Datentransfers angewiesen, um zu kommunizieren, zu reisen und Handel zu treiben. Dies gilt nicht nur, aber besonders für den transatlantischen Datenverkehr. Gleichzeitig brauchen wir bessere Garantien zum Schutz der Bürger. Europa hat auch eine Marktmacht, mit der wir dazu beitragen können, dass die Nichtachtung des Datenschutzes kein Wettbewerbsfaktor bleibt. Nicht in der EU ansässige Unternehmen sollen sich an die EU-Vorschriften halten müssen und die Bürger ihre Rechte in Europa einklagen können.

Wenn wir rasch Erfolg haben wollen, können wir über eine Konzentration der Datenschutzverordnung auf das europäisch dringend Nötige nachdenken: den Bereich der Wirtschaft im digitalen Binnenmarkt. Der Schutz des Bürgers vor staatlicher Datenverarbeitung ist in Deutschland auch dank des Bundesverfassungsgerichts hoch entwickelt. Ihn durch eine weitere europäische Harmonisierung weiter zu verbessern, ist schwer vorstellbar. Als Bundesinnenminister werde ich mich für ein Datenschutzrecht einsetzen, das vor allem internettauglich ist und den Schutz der Betroffenen in den Mittelpunkt stellt. Staat und Bürger sind hier Verbündete. Darüber hinaus müssen wir versuchen, auch in diesem Bereich international gültige Standards zu schaffen."

An Open Letter (21.01.2014) from US Researchers in Cryptography and Information Security

Media reports since last June have revealed that the US government conducts domestic and international surveillance on a massive scale, that it engages in deliberate and covert weakening of Internet security standards, and that it pressures US technology companies to deploy backdoors and other data-collection features. As leading members of the US cryptography and information-security research communities, we deplore these practices and urge that they be changed.

Indiscriminate collection, storage, and processing of unprecedented amounts of personal information chill free speech and invite many types of abuse, ranging from mission creep to identity theft. These are not hypothetical problems; they have occurred many times in the past. Inserting backdoors, sabotaging standards, and tapping commercial data-center links provide bad actors, foreign and domestic, opportunities to exploit the resulting vulnerabilities.

The value of society-wide surveillance in preventing terrorism is unclear, but the threat that such surveillance poses to privacy, democracy, and the US technology sector is readily apparent. Because transparency and public consent are at the core of our democracy, we call upon the US government to subject all mass-surveillance activities to public scrutiny and to resist the deployment of mass-surveillance programs in advance of sound technical and social controls. In finding a way forward, the five principles promulgated at http://reformgovernmentsurveillance.com/ provide a good starting point.

The choice is not whether to allow the NSA to spy. The choice is between a communications infrastructure that is vulnerable to attack at its core and one that, by default, is intrinsically secure for its users. Every country, including our own, must give intelligence and law-enforcement authorities the means to pursue terrorists and criminals, but we can do so without fundamentally undermining the security that enables commerce, entertainment, personal communication, and other aspects of 21st-century life. We urge the US government to reject society-wide surveillance and the subversion of security technology, to adopt state-of-the-art, privacy-preserving technology, and to ensure that new policies, guided by enunciated principles, support human rights, trustworthy commerce, and technical innovation.

Dieser Text und die Liste der 55 Unterzeichner ist auf *http://mass-surveillance.info/* zu finden.

LfD Baden-Württemberg: 31. Tätigkeitsbericht 2012/2013

Der Landesbeauftragte für den Datenschutz, Jörg Klingbeil, hat am 27. Januar 2014 seinen Tätigkeitsbericht vorgestellt, der die Jahre 2012 und 2013 umfasst. Der Bericht im neuen Layout ist – nach der Zusammenlegung der beiden Datenschutzaufsichtsbehörden in Baden-Württemberg zum 1. April 2011 – der zweite seiner Dienststelle, in dem auch der Datenschutz im nicht-öffentlichen Bereich behandelt wird.

Als aktuelle Herausforderungen für den Datenschutz bezeichnete Jörg Klingbeil die Spähaffäre angloamerikanischer Geheimdienste und die zunehmende massenhafte Datenspeicherung und -auswertung für unterschiedliche Zwecke: „Das Jahr 2013 wird als das Jahr in die Geschichte eingehen, in dem das Internet seine Unschuld verloren hat. Die Ohnmacht Deutschlands auf politischer, rechtlicher und technischer Ebene ist durch die NSA-Affäre überdeutlich geworden. Die vom Bundesverfassungsgericht aufgerichteten Schranken (z.B. Grundrecht auf informationelle Selbstbestim-