

PRIVACY TOOLS FOR DATA SHARING

LESSONS LEARNED AND DIRECTIONS FORWARD

RE-CODING PRIVACY LAW

REFLECTIONS ON THE FUTURE RELATIONSHIP AMONG LAW,
TECHNOLOGY, AND PRIVACY

@UGASSER

BERKMAN KLEIN CENTER FOR INTERNET & SOCIETY

DECEMBER 11, 2017





DOMINANT NARRATIVE

TECHNOLOGY

Amazon Echo and the internet of things that spy on you

An upcoming court case could determine the sanctity of what is said between a person and a bot in a home

By Kelsey D. Atherton March 2, 2017

Level of concern for consumers towards the privacy risks of augmented reality in Europe in 2016

[Home](#) > [Information Security](#) > [Privacy](#)

FEATURE

The 5 worst big data privacy risks (and how to guard against them)

There are enormous benefits from Big Data analytics, but also massive potential for exposure that could result in anything from embarrassment to outright discrimination. Here's what to look out for — and how to protect yourself and your employees



Report: Consumers sceptical of AI, fearful of privacy risks


BY JAMES WALKER DEC 7, 2017 IN TECHNOLOGY

[LISTEN](#) | [PRINT](#)

60¢



DO YOU KNOW YOU ARE BEING SPIED ON?
Even as you read this the most
intimate details of your life are being
recorded, bought and
sold by



**THE
PRIVACY
INVADERS**

MYRON BRENTON

"HAIR-RAISING" - The New Yorker

The

Naked
Society

VANCE PACKARD

with an introduction by
RICK PERLSTEIN

ALTERNATIVE READING



Courtesy of IBM



Hessisches Datenschutzgesetz

Das **Hessische Datenschutzgesetz** ist das Datenschutzgesetz für die **öffentliche Verwaltung** des **Landes Hessen**. Es trat 1970 in Kraft und ist damit das erste und älteste **formelle** Datenschutzgesetz der Welt.^[1]

Inhaltsverzeichnis [Verbergen]

- 1 **Gesetzeszweck**
- 2 **Geltungsbereich**
- 3 **Inhalt**
 - 3.1 **Erster Teil: Allgemeiner Datenschutz**
 - 3.2 **Zweiter Teil: Hessischer Datenschutzbeauftragter**
 - 3.3 **Dritter Teil: Besonderer Datenschutz**
 - 3.4 **Vierter Teil: Rechte des Landtags und der kommunalen Vertretungsorgane**
 - 3.5 **Fünfter Teil: Schlussvorschriften**
- 4 **Geschichte**
- 5 **Literatur**
 - 5.1 **Grundlegend**
 - 5.2 **Zur Novellierung 1987**
 - 5.3 **Zur Novellierung 1999**
- 6 **Weblinks**
- 7 **Einzelnachweise**

Basisdaten

Titel:	Hessisches Datenschutzgesetz
Früherer Titel:	Datenschutzgesetz
Abkürzung:	HDSG
Art:	Landesgesetz
Geltungsbereich:	Hessen
Rechtsmaterie:	Datenschutzrecht, Verwaltungsrecht
Fundstellennachweis:	GVBl. II 300-28 ↗
Ursprüngliche Fassung vom:	7. Oktober 1970 (GVBl. I S. 625)
Inkrafttreten am:	13. Oktober 1970
Neubekanntmachung vom:	7. Januar 1999 (GVBl. I S. 98)
Letzte Neufassung vom:	11. November 1986 (GVBl. I S. 309)

[Hauptseite](#)

[Themenportale](#)

[Von A bis Z](#)

[Zufälliger Artikel](#)

[Mitmachen](#)

[Artikel verbessern](#)

[Neuen Artikel anlegen](#)

[Autorenportal](#)

[Hilfe](#)

[Letzte Änderungen](#)

[Kontakt](#)

[Spenden](#)

[Werkzeuge](#)

[Links auf diese Seite](#)

[Änderungen an
verlinkten Seiten](#)

[Spezialseiten](#)

[Permanenter Link](#)

[Seiteninformationen](#)

[Wikidata-Datenobjekt](#)

HARVARD LAW REVIEW.

VOL. IV.

DECEMBER 15, 1890.

NO. 5.

THE RIGHT TO PRIVACY.

"It could be done only on principles of private justice, moral fitness, and public convenience, which, when applied to a new subject, make common law without a precedent; much more when received and approved by usage."

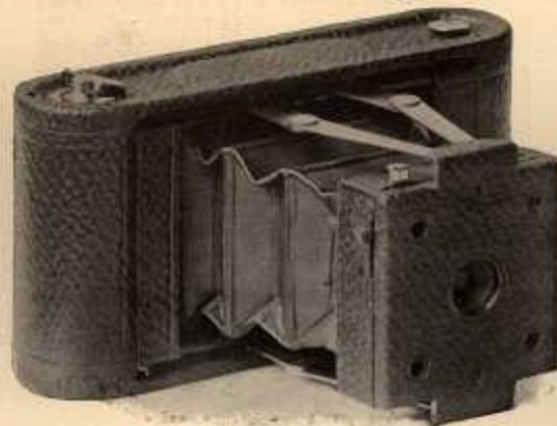
WILLES, J., in *Millar v. Taylor*, 4 Burr. 2303, 2312.

THAT the individual shall have full protection in person and property is a principle as old as the common law. It has been found necessary from time to time to define an exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy for physical interference with life and property, for trespass

There is no Kodak but the Eastman Kodak.

Holidays are Kodak Days

Folding
Pocket
Kodak
\$10.



Indoors and Out the holiday season is a delightful one for amateur photography, making the Kodak an especially welcome Christmas Gift.

exact nature and extent of such protection. Political, social, and economic changes entail the recognition of new rights, and the common law, in its eternal youth, grows to meet the demands of society. Thus, in very early times, the law gave a remedy only for physical interference with life and property, for trespasses *vi et armis*. Then the “right to life” served only to protect the subject from battery in its various forms; liberty meant freedom from actual restraint; and the right to property secured to the individual his lands and his cattle. Later, there came a recognition of man’s spiritual nature, of his feelings and his intellect. Gradually the scope of these legal rights broadened; and now the right to life has come to mean the right to enjoy life,—the right to be let alone; the right to liberty secures the exercise of extensive civil privileges; and the term “property” has grown to comprise every form of possession — intangible, as well as tangible.

CO-EVOLUTION

A Brief History of Information Privacy Law

Daniel J. Solove*

George Washington University Law School

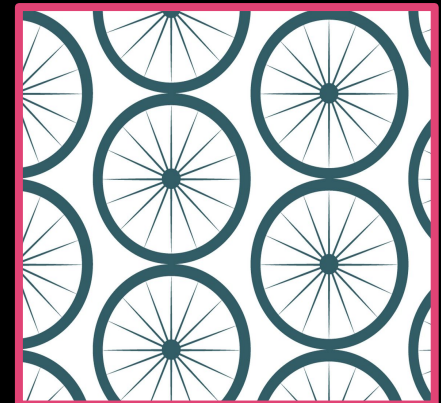
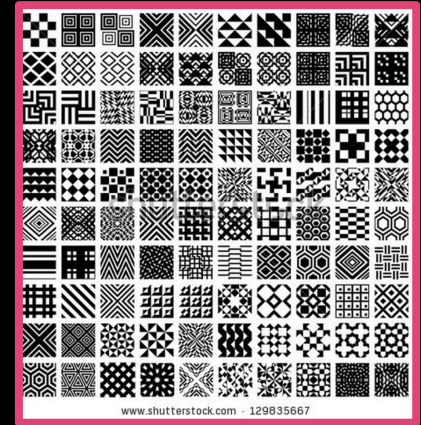
- § 1:1 Introduction
- § 1:2 Colonial America
- § 1:3 The Nineteenth Century
 - § 1:3.1 New Threats to Privacy
 - [A] The Census and Government Records
 - [B] The Mail
 - [C] Telegraph Communications
 - § 1:3.2 The Fourth and Fifth Amendments
 - § 1:3.3 Privacy of the Body
 - § 1:3.4 Warren and Brandeis's the Right to Privacy
- § 1:4 The Twentieth Century
 - § 1:4.1 1900 to 1960
 - [A] Warren and Brandeis's Privacy Torts
 - [A][1] Early Recognition
 - [A][2] William Prosser and the *Restatement*
 - [A][2][a] Intrusion upon Seclusion

- [A][2][b] Public Disclosure of Private Facts
 - [A][2][c] False Light
 - [A][2][d] Appropriation
 - [B] The Emergence of the Breach of Confidentiality Tort
 - [C] The Growth of Government Record Systems
 - [D] The Telephone and Wiretapping
 - [D][1] The Fourth Amendment: *Olmstead v. United States*
 - [D][2] Federal Communications Act Section 605
 - [E] The FBI and Increasing Domestic Surveillance
 - [F] Freedom of Association and the McCarthy Era
- § 1:4.2 The 1960s and 1970s
- [A] New Limits on Government Surveillance
 - [A][1] Fourth Amendment Resurgence: *Katz v. United States*
 - [A][2] Title III of the Omnibus Crime and Control Act of 1968
 - [B] The Constitutional Right to Privacy
 - [B][1] Decisional Privacy: *Griswold v. Connecticut*
 - [B][2] Information Privacy: *Whalen v. Roe*
 - [C] Responses to the Rise of the Computer
 - [C][1] Burgeoning Interest in Privacy
 - [C][2] Freedom of Information Act of 1966
 - [C][3] Fair Information Practices
 - [C][4] Privacy Act of 1974
 - [C][5] Family Educational Rights and Privacy Act of 1974
 - [C][6] Foreign Intelligence Surveillance Act of 1978
 - [D] Financial Privacy
 - [D][1] Fair Credit Reporting Act of 1970
 - [D][2] Bank Secrecy Act of 1970
 - [D][3] *United States v. Miller*
 - [D][4] Right to Financial Privacy Act of 1978
 - [E] The Retreat from Boyd
 - [F] The Narrowing of the Fourth Amendment
- § 1:4.3 The 1980s
- [A] Receding Fourth Amendment Protection
 - [B] The Growth of Federal Privacy Statutory Protection
 - [B][1] Privacy Protection Act of 1980
 - [B][2] Cable Communications Policy Act of 1984
 - [B][3] Computer Matching and Privacy Protection Act of 1988
 - [B][4] Employee Polygraph Protection Act of 1988
 - [B][5] Video Privacy Protection Act of 1988
 - [C] Electronic Communications Privacy Act of 1986
 - [D] OECD Guidelines and International Privacy

- § 1:4.4 The 1990s
 - [A] The Internet, Computer Databases, and Privacy
 - [B] The Continued Growth of Federal Statutory Protection
 - [B][1] Telephone Consumer Protection Act of 1991
 - [B][2] Driver's Privacy Protection Act of 1994
 - [B][3] Health Insurance Portability and Accountability Act of 1996
 - [B][4] Children's Online Privacy Protection Act of 1998
 - [B][5] The Gramm-Leach-Bliley Act of 1999
 - [C] The FTC and Privacy Policies
 - [D] The EU Data Protection Directive
- § 1:5 The Twenty-First Century
 - § 1:5.1 After September 11: Privacy in a World of Terror
 - [A] The USA PATRIOT Act of 2001
 - [B] The FISA "Wall"
 - [C] The Homeland Security Act of 2002
 - [D] The Intelligence Reform and Terrorism Prevention Act of 2004
 - [E] The Real ID Act of 2005
 - [F] NSA Warrantless Surveillance
 - § 1:5.2 Consumer Privacy
 - [A] The Fair and Accurate Credit Transactions Act of 2003
 - [B] The National Do-Not-Call Registry
 - [C] The CAN-SPAM Act of 2003
 - [D] *Remsburg v. Docusearch*
 - [E] Privacy Policies and Contract Law
 - [F] Data Security Breaches
- § 1:6 Conclusion

The legal system has developed different **approaches** to interact with technological changes (“response patterns”):

- **Subsumption**, i.e. application of old rules to new phenomenon (default approach)
- **Gradual responses** over time
- **Innovation**, i.e. enactment of new law (legislator) or introduction of new doctrines (courts)



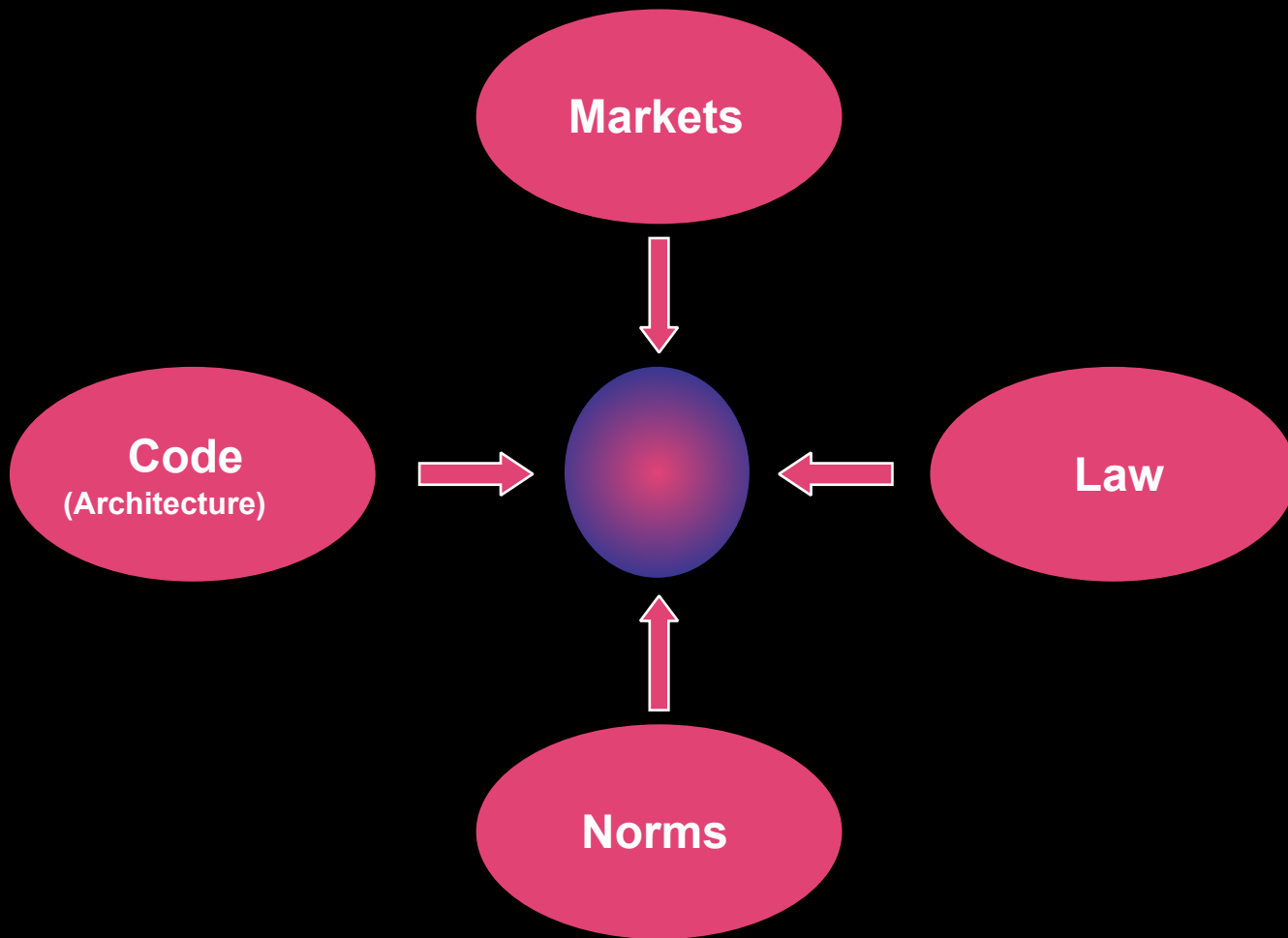
MAY 25TH
2018



GDPR

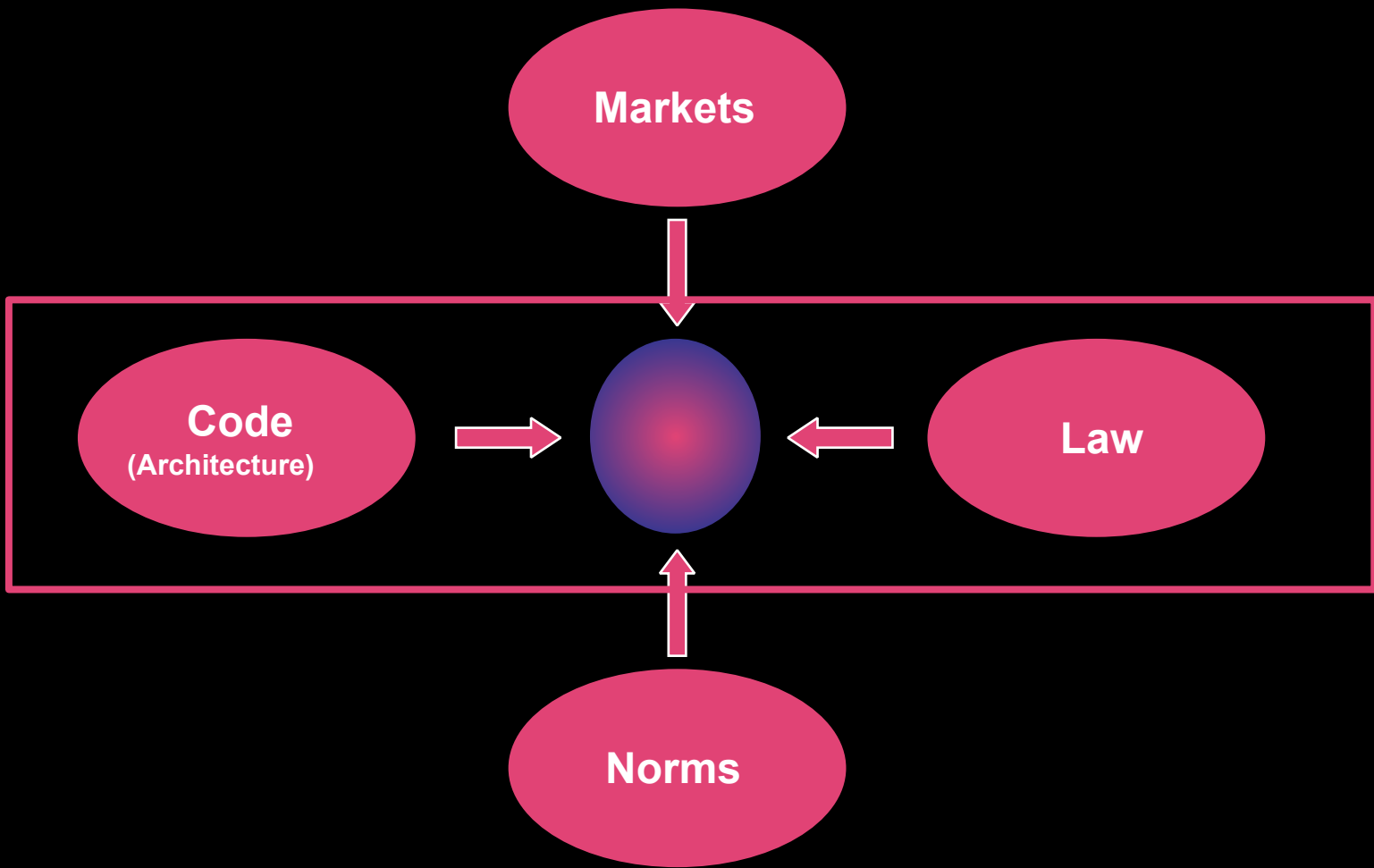


**Privacy
baked in**



Source: Lessig, Code and Other Laws of Cyberspace (1999)

RE-CODING PRIVACY



Source: Lessig, Code and Other Laws of Cyberspace (1999)

Harvard University Privacy Tools Project

[Home](#) [Research ▼](#) [News](#) [People ▼](#) [Publications](#) [Software ▼](#) [Outreach ▼](#)



The Privacy Tools Project is a broad effort to advance a multidisciplinary understanding of data privacy issues and build computational, statistical, legal, and policy tools to help address these issues in a variety of contexts. It is a collaborative effort between Harvard's [Center for Research on Computation and Society](#), [Institute for Quantitative Social Science](#), [Berkman Klein Center for Internet & Society](#), and [Data Privacy Lab](#), and MIT Libraries' [Program on Information Science](#).

LATEST NEWS & BLOG POSTS

[Register for "Privacy Tools for Data Sharing" Workshop on December 11th](#)

[Applications Open for Summer 2018 Research Opportunities](#)

[CRCS Call for Postdoctoral Fellows and Visiting Scholars](#)

[Michael Bar-Sinai Presents PolicyModels in Demo at FORCE2017](#)

[Privacy Tools Team Members among the Organizers and Speakers at DIMACS Workshop on Barriers to Data Sharing](#)

[Privacy Tools Team Members' Abstract Accepted for Publication at 2017 Brussels Privacy Symposium](#)

[Privacy Tools Team Member Alex Wood to Present at HHS Symposium 2017](#)

[Privacy Tools Team Members to Present at](#)

These developments might ultimately culminate in a more deeply layered recoding of privacy law that leverages the synergies between technological and legal perspectives and instruments and transcends the traditional response patterns discussed earlier in this Commentary in order to cope with the complex privacy-relevant challenges of our future. For example, in light of substantial definitional gaps between various technological and legal approaches to privacy, updating the law to better support new privacy technologies could require a fundamental reframing away from traditional legal notions such as “Personally Identifiable Information”³¹ and “de-identification.”³² Furthermore, legal standards could be redesigned to focus on the ends rather than the means of privacy protection, which are likely to continue to evolve rapidly. Rather than implicitly or explicitly endorsing traditional approaches like de-identification, updated legal standards might, for instance, adopt more general descriptions of the intended privacy goal, which would provide a clearer basis for demonstrating whether new classes of emerging privacy technologies are sufficient.

par·a·digm shift

noun

noun: **paradigm shift**; plural noun: **paradigm shifts**

a fundamental change in approach or underlying assumptions.

Origin

1970s: term used in the writings of Thomas S. Kuhn (1922–96), philosopher of science.

privacy

Via:

 Program on Information Science
MIT Libraries

 **CRCS** Center for Research on
Computation and Society

social
science

 **IQSS**
The Institute for Quantitative Social Science
HARVARD UNIVERSITY

computer
science

data science

 **BERKMAN KLEIN CENTER**
FOR INTERNET & SOCIETY AT HARVARD UNIVERSITY

law &
policy

 **DATA PRIVACY LAB**

NEXT FRONTIERS

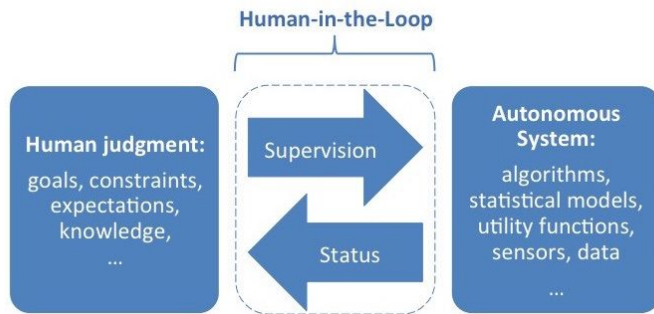
Society-in-the-Loop

Programming the Algorithmic Social Contract

MIT Media Lab director [Joi Ito](#) recently published a thoughtful essay titled “[Society-in-the-Loop Artificial Intelligence](#),” and has kindly credited me with coining the term. Now that it is out there, I wanted to elaborate a little on what I mean by “society in the loop,” and to highlight the gap that it bridges between the humanities and computing.

Human-in-the-Loop

What I call “society in the loop” is a scaled up version of an old idea that puts the “[human in the loop](#)” (HITL) of automated systems. In HITL systems, a human operator is a crucial component of a control system, handling challenging tasks of supervision, exception control, optimization and maintenance. Entire fields of study focus on how to best engineer HITL systems to optimize performance, making the most of human judgment while avoiding human limitation, such as susceptibility to information overload, or systematic cognitive bias.



VIEWPOINT

Designing AI Systems that Obey Our Laws and Values

By [Amitai Etzioni, Oren Etzioni](#)
Communications of the ACM, Vol. 59 No. 9, Pages 29-31
[10.1145/2955091](#)
[Comments \(2\)](#)

VIEW AS: SHARE:



Operational AI systems (for example, self-driving cars) need to obey both the law of the land and our values. We propose AI oversight systems (“AI Guardians”) as an approach to addressing this challenge, and to respond to the potential risks associated with increasingly autonomous AI systems.¹ These AI oversight systems serve to verify that operational systems did not stray unduly from the guidelines of their programmers and to bring them back in compliance if they do stray. The introduction of such second-order, oversight systems is not meant to suggest strict, powerful, or rigid (from here on ‘strong’) controls. Operations systems need a great degree of latitude in order to follow the lessons of their learning from additional data mining and experience and to be able to render at least semi-autonomous decisions (more about this later). However, all operational systems need some boundaries, both in order to not violate the law and to adhere to ethical norms. Developing such oversight systems, AI Guardians, is a major new mission for the AI community.

SIGN IN for Full Access

User Name

Password

[» Forgot Password?](#)

[» Create an ACM Web Account](#)

SIGN IN

ARTICLE CONTENTS:

[Introduction](#)
[Terra Incognita](#)
[Different Kinds of AI Guardians](#)
[Interrogators](#)
[Who Will Guard the AI Guardians?](#)
[References](#)
[Authors](#)
[Footnotes](#)

THANK YOU