

What are your rights to privacy in the IoT? Many systems can be used for both good and ill: Video surveillance may be tremendously helpful in allowing senior citizens stay in their homes longer and parents to monitor their newborns; they can also expose private behavior to unscrupulous viewers and unwanted intrusion. Some have suggested that individuals should have a basic right to opt out, delete, or mask their information from systems in the IoT, providing one tenet of a potential IoT "Bill of Rights." However, it may be infeasible or impossible for an individual to control all the data generated about them by IoT systems. Interestingly, strong individual privacy rights may also mean less social benefit. Too many "opt-outs" may erode the public and private value of IoT datasets,³ negatively impacting their social benefit—imagine a Google map where locations come and go. The complexity of providing useful services subject to dynamic participation and evolving individual preferences may be extraordinarily complex to develop and administer. Will we need to develop and incorporate "artificial ethics" into automated systems to help them respond in environments when there are good and bad choices? If so, whose ethics should be applied? Toward a Framework for Thinking About Principles and Policy for the IoT

What might a general IoT governance model look like? In 2008, the Forum for a New World Governance developed the "World Governance Index" (WGI) focusing on peace and security, democracy and the rule of law, human rights, development and participation, and sustainability. As IoT technologies become more pervasive, personal information will become more valuable to a diverse set of actors that include organizations, individuals, and autonomous systems with the capacity to make decisions about you. Sustainable development of the IoT as part of a larger societal and technological ecosystem, including its impact on biological systems (for example, 3D-printed organs, implants), environmental systems, and natural resources). The first step is to pursue the discussions, studies, task forces, commissions, and pilots that will help develop governance for an empowering and enabling IoT. Policy for IoT safety, security and privacy, requiring the development of viable approaches promoting individual rights, data security, and trust, as well as disincentives and penalties for inappropriate behavior, corruption, and crime. In his highly popular and visionary books, Isaac Asimov posited four laws of robotics^{1,2} on the basic theme that robots may not harm humans (or humanity), or, by inaction, allow humans (humanity) to come to harm. The IoT will sharpen the tension between individual privacy and the use of personal information to promote effectiveness, safety, and security.^{2.3.???}