

The convergence of technologies, generates convergence in the regulations

Guillermo Valdes Mesa

Havana University Center Biomaterial, Cuba

Abstract

The convergence of nanotechnologies generates synergies among different technologies to say, nanotechnologies, neurotechnology, computers and biotechnology, these technologies must converge it's their regulations, the application of medical devices in nanotechnologies should lead us to a link between the technical committee TC 210 and ISO technical committee 229 link that does not exist in our work in this moment In this do an analysis of the management of risk from an optical NC-ISO 14971. Studying the global trend in this respect as imported for manufacturers medical Devices worldwide. The convergences of technologies are a consequence of atomic precision, where the boundary between the biotic and abiotic mute blur the interaction. The interaction between nanotechnologies, biotechnology and informatics and communications (NBI) generates a synergy of unusual consequences of all is known that the industry of semiconductor)s is the one of greater precision that is atomic, the new medical devices that will be applied in the teranocis will dose Physical principles that will be governed under the laws of quantum mechanicsbut there are two problems that have not been solved even though they are one the non-existence of quantum biology and the transition from quantum to classical mechanics. On the other hand, the redefinition of the international system of units based on the universal constants that will be implemented by 2019 has a deficiency that is the second that redefines implies redefinition of the meter the chain of traceability proposed for nanometrology presents a serious difficulty when putting the microcopy of atomic force wing of effect tunnel situation that is changing the verification of the Wiedemann-Franz law at atomic level yields a result where the phononic component is taken into account, a result that launches STM to the cusp of the chain of traceability above inclusive of interferometry.

Technological convergence, in general, refers to the trend or phenomenon where two or more independent technologies integrate and form a new outcome. One example is the smartphone. A smartphone integrated several independent technologies—such as telephone, computer, camera, music player, television (TV), and geolocating and navigation tool—into a single device. The smartphone has become its own, identifiable category of technology, establishing a \$350 billion industry.

Of the three closely associated convergences—technological convergence, media convergence, and network convergence—consumers most often directly engage with technological convergence. Technological convergent devices share three key characteristics. First, converged devices can execute multiple functions to serve blended purpose. Second, converged devices can collect and use data in various formats and employ machine learning techniques to deliver enhanced user experience. Third, converged devices are connected to a network directly and/or are interconnected with other devices to offer ubiquitous access to users.

Technological convergence may present a range of issues where Congress may take legislative and/or oversight actions. Three selected issue areas associated with technological convergence are regulatory jurisdiction, digital privacy, and data security. First, merging and integrating multiple technologies from distinct functional categories into one converged technology may pose challenges to defining regulatory policies and responsibilities. Determining oversight jurisdictions and regulatory authorities for converged technologies can become unclear as the boundaries that once separated single-function technologies blend together. A challenge for Congress may be in delineating which government agency has jurisdiction over various converged technologies. Defining policies that regulate technological convergence industry may not be simple or straightforward. This may further complicate how Congress oversees government agencies and converged industries due to blending boundaries of existing categories.

Second, converged technologies collect and use personal and machine data which may raise digital privacy concerns for consumers. Data collection and usage are tied to digital privacy issues because a piece or aggregation of information could identify an individual or reveal patterns in one's activities. Converged or smart technologies leverage large volumes of data to try to improve the user experience by generating more tailored and anticipatory results. However, such data can potentially identify, locate, track, and monitor an individual without the person's knowledge. Such data can also potentially be sold to third-party entities without an individual's awareness. As the use of converged technologies continues to propagate, digital privacy issues will likely remain central.

Third, data security concerns are often associated with smart devices' convenient ubiquitous features that may double as vulnerabilities exploited by malicious actors. Data security, a component of cybersecurity, protects data from unauthorized access and use. Along with digital privacy, data security is a pertinent issue to technological convergence. As converged devices generate and consume large volumes of data, multiple data security concerns have emerged: potentially increased number of access points susceptible to cyberattacks, linkage to physical security, and theft of data.

Relatively few policies are in place for specifically overseeing technological convergence, and current federal data protection laws have varied privacy and data security provisions for different types of personal data. To address regulatory, digital privacy, and data security issues, Congress may consider the role of the federal government in an environment where technological evolution changes quickly and continues to disrupt existing regulatory frameworks. Regulating technological convergence may entail policies for jurisdictional deconfliction, harmonization, and expansion to address blended or new categories of technology. One approach could be for Congress to define the role of federal government oversight of digital privacy and data security by introducing new legislation that comprehensively addresses digital privacy and data security issues or by expanding the current authorities of federal agencies. When considering new legislation or expanding the authorities of federal agencies, three potential policy decisions are (1) whether data privacy and data security should be addressed together or separately, (2) whether various types of personal data should be treated equally or differently, and (3) which agencies should be responsible for implementing any new laws.