

<http://idcubed.org>

About

ID3 Open Source Software

Projects

Idea Streams (<http://idcubed.org/personal-data-ecosystem>)

Digital Law

Get Involved (<http://idcubed.org/network>)

The Rise of Digital Common Law

An Argument for Trust Frameworks, Digital Common Law and Digital Forms of Governance

By John Henry Clippinger and David Bollier

© ID3 2012

As more of life and commerce are mediated by digital technologies and Internet platforms, the tensions between legacy institutions (centralized, hierarchical, control-based) and emergent social practices on open networks (distributed, participatory, emergent) are intensifying. For years, such tensions have been deliberately ignored or finessed – but that approach may no longer be possible. The structural deficiencies of existing online systems are spurring the search for better, more practical approaches to governance, law and policymaking in an age of open networks.

For many reasons conventional government policymaking is increasingly unable to provide timely, responsive, and effective governance and policymaking. The process itself is paralyzed by a political gridlock in the U.S. Congress that shuns evidence-driven policymaking; by complexity and delays in law-making, regulation and litigation; by the “pay to play” ethic that has tainted the legitimacy of governance; by cumbersome and ineffectual enforcement systems; and by the sheer expense of relying upon lawyers to protect one’s interests. Conventional policymaking, an artifact of an 18th Century constitution and 20th Century bureaucracy, is also ill-equipped to deal with the radically different foundational space of digital activities – an “alternative reality” that is instantaneous, non-territorial and constantly evolving. In a sense, human activity has migrated to a different dimension of life that is far less amenable to control through conventional government and legal systems.

There are a growing number of serious initiatives seeking to improve the security of identity management, the ease of data storage in the cloud, the interoperability and use of large databases, and the trustworthiness of social networking. ID3 hopes to instigate a new conversation that can begin to integrate many of these concerns into more coherent, dynamic solutions. We wish to explore how we might develop a new set of network protocols and software platforms that could blend software

design, legal governance, market incentives, and user-centric action into a stable new type of ecosystem. In its most ambitious sense, we are talking about the next, great leap in the structure of the Internet and its socio-legal-economic evolution.

The ultimate goal is to develop a networked architecture for personal data that will enable new forms of trusted governance, commercial transactions, and social relationships. The envisioned system would seek to leverage the powers of Big Data while empowering users to control how their personal information can be used. By helping devise a more transparent, accountable governance system that is holistic in scope – and only minimally dependent upon legacy institutions of law and policymaking – we hope to nurture a new, network-native form of law that we call digital common law.

Many complex and interconnected questions must be addressed in building this infrastructure and in developing the socio-legal-technical framework for digital common law. Among the major questions are how to set policies for socially acceptable uses of large, interlinked databases; how to provide digital security and authentication for open networks; and how to assure user control over personal information in an ocean of commercially valuable Big Data. A key tool for answering these questions, we believe, is what National Strategy for Trusted Identities in Cyberspace (NSTIC) calls Trust Frameworks – a set of consensual, multi-stakeholder contractual agreements to enable people to enter into trustworthy relationships and transactions on open networks.

Such a system is needed because conventional forms of law and policymaking are ultimately too ham-fisted, slow moving, impractical and unenforceable to address the robust needs of commerce and social life on open networks. In a sense, law itself must be re-conceptualized if it is to function well in networked environments. Now is the time to engineer a great leap forward to digital, network-native forms of law, where the rule of law derives from the collective sentiments of a given community or network of users and functions in a more algorithmic, self-executing and self-correcting way.

At first blush, this idea may sound unrealistic, radical, or ridiculous. But we believe that this vision is entirely feasible and, indeed, highly attractive, because it can begin to solve so many vexing social, economic and technological problems that existing institutions and policy structures cannot. This discussion paper outlines the key design elements of the envisioned network platform and explains the basic logic of the infrastructure and digital common law.

Design Principles for Governance on Open Networks

We need to entertain new sorts of “digital law” because networked computing is reaching new thresholds of scale, sophistication and ubiquity. Thanks to inexpensive digital memory and growing interconnectivity, massive databases are now proliferating in the cloud, providing unprecedented dangers for privacy violations and security breaches. New developments in machine learning are turning our physical and social environment (buildings, urban spaces, motor vehicles, personal products) into a flexible, “smart” infrastructure. This infrastructure is increasingly “getting to know us” by aggregating our personal preferences and those of our peer groups.

While these developments are opening up rich new opportunities for innovation and commerce, legislatures, regulatory agencies, and courts are ill equipped to provide the kinds of governance, legal structures and political accountability that are needed. Bridging this growing mismatch between

conventional governance and digital opportunities is an urgent priority. ID3 wishes to explore the necessary characteristics of a new software infrastructure and set of network protocols that could leverage the enormous value proposition of open networks while assuring necessary forms of governance, law, and accountability. We believe that such a system could be built by combining many existing software systems and exploiting cutting-edge innovations to leverage the power of Big Data and machine learning – all in conformance with consensus policy recommendations for assuring privacy and security.

A software platform of this sort would have the following features:

- Users could set the terms for controlling their personal data, including portability, consistent with the Obama administration's Data Bill of Rights and EU policies;
- The latent value of Big Data could be harnessed for positive economic and social ends through new sorts of "personal data ecosystems";
- Security and privacy would be embedded in the network design, and would not require costly and complicated external enforcement (government action, litigation, etc.);
- The prime driver of value-creation would be open sharing and collaboration in an open, competitive marketplace rather than a winner-take-all marketplace whose dominant players set the terms of innovation and competition;
- Online communities would have autonomy in governing how collaboratively created value will be stewarded and allocated; and
- The infrastructure design would enable trustworthy relationships and permeable organizational boundaries to flourish in networked spaces.

A platform with these characteristics could provide a functional architecture for managing online identity, security, data, and collective governance in an integrated fashion. It could demonstrate that privacy-enhancing technologies are compatible with and highly supportive of viable business models, effective security requirements and generally accepted performance standards. By dealing with a range of urgent issues in a holistic manner, the platform could unleash new forms of high-value, networked-based services that are being needlessly stymied by archaic business models, conventional public policies and, indeed, by the existing policymaking process itself. We envision that such a platform could also conform to principles set forth by NSTIC, and the general principles for digital privacy, security, and user control identified by the EU and other governments.

Digital Common Law

The new platform amounts to a new sort of socio-legal-technical governance regime. Digital common law, as we call it, is a bottom-up, voluntary, user-driven system that establishes context-specific norms for governing a given online community/market. While broad parameters of law continue to be set by legislatures, executive branch agencies and courts, the point of this social-legal-technical ecosystem is to embed as many fundamental principles of decision-making, oversight, and enforcement as possible into the software design and network protocols themselves.

We consider this a natural progression in the evolution of law. A system once based on oral, social forms and then later written, institutional forms must move into the digital realm and become algorithmic. That is to say, it makes sense in the digital age for people to use self-learning, data-driven network computing as instruments of law. They can provide a reliable, effective way to identify and represent collective sentiment, and to oversee and enforce such sentiments. The basic principle of digital common law is to use open network systems to formalize mutual accountability and shared intentions. Distinct communities and/or participants on open networks can invent and define their own operational norms to suit their needs, subject to general public policy mandates. The system can be highly attentive to shifting circumstances and preferences, and make suitable modifications without the impediments that afflict conventional law and policy.

Digital common law is not a fanciful idea, but an eminently practical and attractive idea now that so much commerce and everyday life occurs on digital platforms. As noted, conventional government has trouble effectively legislating and regulating digital activities because it cannot keep up with their faster innovation cycles and fast-changing social norms. Government antitrust lawsuits, for example, can take years to resolve, by which time remedies for the entire original offense may have limited or counterproductive impact. Privacy regulation, too, can take a long time and be fraught with uncertainties, which in turn provoke an elaborate collective gaming of the process rather than straightforward regulation and compliance.

To be sure, digital structures will not displace government; there will continue to be a need for antitrust law, privacy regulation, consumer protection, and so forth. But digital structures can enable new types of consensual governance that will almost certainly be more flexible, effective, and evolvable than existing structures. By moving from a system of external regulation focused on compliance and punishment to one that internalizes feedback and governance into the (digital) system itself, we can expand the “solution space” for effective regulation. In many circumstances, too, digital common law will be seen as more responsive and socially legitimate than existing systems of law and policy. It can avoid the huge costs, uncertain liabilities, and problematic social acceptance of government policymaking, while providing a hosting infrastructure on which more adaptive, context-specific and politically neutralized solutions can emerge. The idea is to use open networks to “learn” from user behaviors and databases, and to let systems self-organize their own innovative responses over time.

If the contours of digital common law and its institutions remain a bit fuzzy, it is precisely because the goal of an open platform is to evolve these new forms over time through user participation, much as the World Wide Web, open source software, and countless other network-based ecosystems have evolved in unexpected ways through mass participation. Digital common law regards governance institutions as emergent systems that will arise through repeated experimentation and tests animated by the social ingenuity and mores of users. As a self-organized project, it will embed principles of transparency, integrity, and accountability into the system itself; such principles tend to make social governance regimes more legitimate, stable, and self-sustaining. The infrastructure that we envision will naturally elicit diverse sorts of experiments in a variety of venues; from this process, consensually acceptable rules, social norms and institutions will emerge. On such an open, exploratory platform,

governance modalities will have less to do with traditional ideologies or jurisprudence than with their sheer functionality and user acceptability. What matters is that “the consent of the governed” will be richly served by the co-construction of governance rules by participants themselves.

This practice-based approach draws directly upon Oliver Wendell Holmes, Jr.’s classic critique of common law as a generative, self-correcting process, and upon the anthropologist Claude Lévi-Strauss’ notion of bricolage as a process of constructing something new from whatever exists at hand. In his 1881 essay, “The Common Law,” Holmes noted, “The first requirement of a sound body of law is that it should correspond with the actual feelings and demands of the community, whether right or wrong.” One of the great virtues of common law has been precisely that it is based on disaggregated real-world experiences and the accepted social customs of ordinary people. It can therefore evolve and mutate as new conditions arise while still reflecting the sentiments of ordinary people in their actual local circumstances. This insight led to Holmes’ famous passage: “The life of the law has not been logic; it has been experience. The felt necessities of the time, the prevalent moral and political theories, intuitions of public policy, avowed or unconscious, even the prejudices which judges share with their fellow-men, have had a good deal more to do than the syllogism in determining the rules by which men should be governed.” Lévi-Strauss’ notion of bricolage astutely captures the basis of so much Internet-based creativity today, and yet reflects the animating principle of common law, as described by Holmes.

As digital technologies become smarter and more interconnected, we need a network infrastructure that can enable self-organized, bricolage-style governance: a digital common law. Instead of a strict adversarial system that assumes most of the burden for identifying misdeeds and imposing punishments, we need a system that welcomes trial-and-error experimentation and learning, and then aggregates feedback and errors in order to point register progress in advancing toward consensual “goal sets.” When self-corrections are integrated into the granular, everyday activity of a community, any “sanctions” are experienced more as gentle peer corrections and admonishments, and less as formal, law-driven punishments. Such a system is more robust and efficient because it welcomes an ongoing process of experimentation, feedback, and testing in the context of local conditions, while generalizing rules as possible. If the algorithmic bases of the digital common law are sufficiently refined, any external oversight, regulation or voting becomes moot. The system automatically yields clear signs when one method works better than another, and when one approach has greater social acceptance while others are reviled. The real challenge, then, takes place at a meta-level: designing the right combination of metrics for identifying and validating a group’s online behavior, and enabling social practice and digital common law to co-evolve over time.

Trust Frameworks and Trust Wrappers

No system of digital common law can work unless it enables the members of a community to develop social trust among themselves and the institutions with whom they deal. This process begins with each participant having the capacity to control information about themselves and to select how much they will disclose about themselves to others – businesses, government, social and civic groups, family, and friends. Participants must also have the ability to choose how to share and whether to monetize their data.

We are developing a Trusted Data Governance Infrastructure (TDGI) that allows people to store, access and share their personal data in “personal data lockers” that have multiple rings of protection and no single-point solution for gaining access. By providing far more secure access and only under specified conditions, the TDGI can facilitate a new kind of legally sanctioned “liquidity” in data. This, in turn, clears the way for data to drive all sorts of innovative business models and social collaborations.

The tool that enables digital common law to arise and express the bottom-up, social experience of a community is the trust wrapper. This is a locally adaptable software module that enables individuals to enter into relationships with absolute assurance that their digital identities, privacy, and security will be protected under terms they can personally shape and control. Trust wrappers can be used as an access control system for any digital artifact. They let people enter into and maintain trusted relationships on open networks, including Trust on First Use (TOFU) – and this, in turn, lets new sorts of communities and markets arise on open networks with a bare minimum of external systems of law and policy. Communities that use Trust Frameworks can customize the management of data, digital identities, and transactions in secure, reliable ways.

Certainly governments and international agencies could insert themselves into how specific trusted infrastructures are governed and interoperate, by issuing warrants, enforcing regulations, and so forth. But from an architectural perspective, the TDGI would be wholly independent of government and business in order to assure that it is efficient, trusted, and accepted. Its open architecture would be designed to advance the fiduciary interests of all individuals and groups who own the data. It would also incentivize technology and legal innovation, and prevent the capture of the infrastructure by any government, agency, syndicate, business, or special interest.

Trust Frameworks can be seen as a private-law substitute for conventional systems of law – one that participants actively design and consent to, among other possible choices. Trust Frameworks make the entire law-making and -enforcement process an organic feature of the community itself, blending it with the social practices, norms, and ethos of the community. As a result, the enormous frictions caused by inapt, unjust, or special-interest-driven laws can be reduced or eliminated. Clarity and predictability in the law are greatly improved, and social motivations and enforcement of rules are brought into greater alignment. The upshot: an unleashing of productive participation and innovation on open networks, and an avoidance of social resistance, demoralization, and blockages.

A New Vision of Network-Native Governance


The virtue of using Trust Frameworks to “discover” and evolve digital common law within a given community is that it internalizes law into the very transactional structures of online life. The built-in monitoring, governance, dispute resolution, enforcement, and auditing engender more responsive and stable forms of governance. People are more likely to respect and participate in a system whose governance procedures are transparent and responsive, and that enables the positive externalities generated by a community to be captured for collective (and personal) benefit.

By internalizing certain principles of governance and law into the platform itself and providing auditable enforcement and accountability, the envisioned infrastructure bypasses many of the structural limitations of contemporary public policymaking. It empowers user-communities themselves to set the

terms of information disclosures and sharing. They can allocate rights, duties and other group privileges as they see fit. Because the infrastructure is a set of open, non-proprietary protocols and software systems, it can constantly evolve and virally propagate itself through global networks. It will also have the modularity and self-organizing flexibility that the TCP/IP protocols have provided to the Internet itself. Therefore its adoption will be directly proportional to its utility in serving the needs of user communities and securing their trust and acceptance.

This platform abandons the classical-modernist system of bureaucratic oversight and control, and instead leverages the demonstrated capacity of people on open platforms to self-organize themselves into collaborative regimes that can organize stable communities, mediate conflicts, and get real work done. In this regard, Trust Frameworks emulate open-source and Creative Commons licenses in enabling collaborative value to emerge more readily and in ways that are shareable and protectable. Yet Trust Frameworks expand these capabilities in a far richer, more robust way because they provide a more versatile, subtle infrastructure for open collaboration.

[Back to top](#) [Team \(http://idcubed.org/team\)](http://idcubed.org/team) [Careers \(http://idcubed.org/careers\)](http://idcubed.org/careers) [Contact \(http://idcubed.org/contact\)](http://idcubed.org/contact)

 (http://creativecommons.org/licenses/by-sa/3.0/deed.en_US) This work is licensed under a [Creative Commons Attribution-ShareAlike 3.0 Unported License \(http://creativecommons.org/licenses/by-sa/3.0/deed.en_US\)](http://creativecommons.org/licenses/by-sa/3.0/deed.en_US).