CIVICS.com Consultancy

.Data + Identity = Results

- Systems Design & Architecture
- Entrepreneurship & Innovation
- Public Service & Contribution

- About
- Blog
- Gallery

The Trust Stack

admin · January 5, 2015

> "This post is a work in progress, being drafting to describe the method and mechanisms called a "Trust Stack". The IDfederation.org's "SignOn Once" initiative is a good example of how the Trust Stack can be applied to enable critical but complex industry-wide technical innovation."

The conceptual layers of a "Trust Stack" are intended to enable visualization of the building blocks upon which reasonable reliance is premised. This design and modeling approach provides a powerfully effective method for building reliable high volume transaction systems. The foundations of a Trust Stack are built on the bedrock of existing roles, relationships and other sources of common expectations of parties who do or will participate in a given online system.

An excellent encapsulation of the Trust Stack concept was offered by Dwight Arthur at the peak of the PKI wave. Speaking to a large group of stalwart PKI advocates on a key standards setting email list, Dwight Arthur wrote, in relevant part:

…On the contrary I would suggest that in many cases the RP represents an enterprise that causes a certificate to be granted because of a pre-existing relationship of trust. In other words, trust leads to certificates, certificates do not lead to trust. http://www.ietf.org/mail-archive/web/pkix/current/msg23560.html

The above view, expressed in January of 1998, is just as relevant today some 15 years later. Today, the exciting technology is federated identity for mass-scale "single sign-on" and the related "claims-based" grants of authorization for data access and other permissions. These federated and claims-based technologies have demonstrated capability for wide-scale use and a remarkable capability of achieving better security, lower costs and greater usability for end-users than the alternatives. It is clear that these types of technologies hold the potential to enable wholly new types of transactions, previously impossible insights and predictions based on data as well as the second order transformation through novel markets, professional fields, academic disciplines and other societal transformations. And yet, at this point in time, the technology on it's own does not create meaningful "trust" any more than PKI did. The need for a business relationship between parties that has value in and of it's own right continues, and the technology can be leveraged by insightful and innovative business champions to provide better value to customers and hence expand and retain those business relationships.

I recently posted on Google+ on this concept as well (if you look at the google+ post, you need to click "expand post" to see all the content, and this bit on this topic is mostly in the third paragraph). Based on feedback and inquiries to day, it seemed that creating an anchor URL for the notion here at CIVICS.com would be a good way to accumulate the various resources and conversations bubbling up on the topic. I'll be updating this page from time to time with links or info about relevant resources that come my way. Meanwhile, if you have ideas or perspectives about the Trust Stack concept, please share your input and let's broaden the dialog.

ABA Digital Signature Guidelines

Dazza Greenwood · January 5, 2015

TITLE: Digital Signature Guidelines

LINK: http://www.abanet.org/scitech/ec/isc/dsgfree.html

OVERVIEW: This seminal document by the Information Security Committee of the ABA describing the then novel concept of a "Digital Signature", which is a legal signature of a person effectuated by use of a cryptographic process. These guidelines outline in some detail the legal and process requirements then thought necessary to create a reliable enforceable signature.

ROLE: As a member of the Information Security Committee I was a contributing author to this document and also held meetings of state governments to share relevant information and practices related to the use of Digital Signatures.

Comment

Uniform Law Governing Bots

Dazza Greenwood · January 5, 2015

> "Contribution to Drafting of Uniform Law Governing Electronic Agents and Automated Transactions Using Electronic Signatures, Contracts and Other Records (ie: Law on Bots)"
>
> — http://www.uniformlaws.org/shared/docs/electronic%20transactions/ueta_final_99.pdf

---

M E M O R A N D U M

To: Uniform Electronic Transactions Act Drafting Committee; Professor Patricia B. Fry, Chair and Professor Benjamin Beard, Reporter

From: ABA Section of Business Law, Cyberspace Law Committee Electronic Commerce Subcommittee Working Group on Electronic Contracting Practices Co-Chairs: Daniel Greenwood and John Muller (fn1)

Date: February 16, 1999

Subject: Preliminary Draft Report on UETA Legal Treatment of Electronic Agents

1. Introduction

This document is a revised draft (fn2) of the meeting proceedings of the Electronic Contracting Practices Working Group at the American Bar Association's Cyberspace Law Committee meeting in Atlanta January 15-16, 1999. The Working Group is focusing its efforts on a survey of legal

issues arising from the deployment of electronic agents for business purposes, including considerations of commercial, agency, intellectual property and tort law. As part of this survey, the Working Groups is monitoring and commenting upon developments in UCC Articles 2, 2B and the UETA with respect to Electronic Agents. An initial rough draft of this document was presented on January 16th to Benjamin Beard, UETA Reporter, who has subsequently requested a more formal submission for consideration by the UETA drafting committee in time for the upcoming February 19-21, 1999 drafting Committee meeting in Richmond, VA.

This document first explores the definition currently used in the UETA for Electronic Agent, and then examines the core operative legal rule in the current and immediately prior draft of the UETA, along with a tentative proposed rule developed by the Working Group at the Atlanta meeting. Next, the extent to which operations of an electronic agent should be attributed to a user are discussed, followed by a query about the advisability of developing different operative rules for tool-like vs. intelligent electronic agents (or, possibly, simply limiting application of the UETA to non-intelligent systems). Clearly, other sections of the UETA as well as other NCCUSL draft products also deal with use of electronic agents, however, at this time the Working Group has limited comments to the provisions noted due to the preliminary nature of this draft.

2. UETA Definitions

January 29, 1999 UETA definition of electronic agent (Section 102(8)):

"Electronic agent" means a computer program, electronic, or other automated means used to initiate or respond to electronic records or performances in whole or in part without review by an individual.

Working Group commentary: The emphasis in the definition on review by an individual may call for clarification that review occurring at any point after completion of the record or performance does not cause a program to fall outside this definition. Perhaps this should be clarified with reference to an objective standard, such as: "without human review up to and including the point at which a reasonable person would have expected the transaction to be concluded." It has also been pointed out to the Working Group that (absent the artificial intelligence or malfunction), the future authorized operations of an electronic agent are in fact "reviewed" at the time the user enters the "input" (e.g. enters: "buy 5 shares of X stock at market value").

Query whether "inputs" and/or "outputs" are a preferable term to "performances" because any real world performances (such as shipping goods) are really the result of computer input or output.

3. Alternative Operative Legal Provisions

Prior UETA Treatment: "A person who configures and enables an electronic device is bound by operations of the device."

Working Group Atlanta Meeting Suggestion: "A person may act through an electronic device, and the resulting operations of that device are the acts of that person."

Current UETA Treatment: Operations of an electronic agent are the acts of a person if the person used the electronic agent for such purposes.

4. Attribution of an Electronic Agent's Operations to the User

The Working Group strongly supports the move in the current draft of the UETA away from the wording that the user of an electronic agent is "bound" by the agent, and towards a simpler attribution rule that the acts of an agent are deemed to be the acts of the person who chose to use the

agent, subject to all of the defenses that would be available to the person under existing substantive rules of law. Baldly legislating that a person is to be legally "bound" by the act of an agent strongly suggests a liability and risk allocation rule of strict liability. The scope of application of the UETA is broad enough to raise significant concerns over such a rule. For example, if the underlying transactions gave rise to contract or negligence claims, then application of such a harsh rule would seem out of place because these underlying bodies of law take into account various "escape valves" that allow avoidance of liability under certain circumstances. For example:

Contracts: For example, there exists a contract law doctrine that "a reasonable person would have concluded that an offer had been made" as a condition of the right to accept. The user of an agent that entered an order for 100,000 widgets when the purchaser had regularly purchased quantities of no more than 1,000 should be able to avail herself of this rule.

Negligence: Similarly, under tort law, the user may be able to establish the she met a reasonable level of care which a user must take regarding supervision of its e-agent's actions, and beyond which the user is exculpated

Agency: Under agency law, principals may avoid contract liability for an agent's acts if (i) the agent acts outside its scope of authority, or (ii) if apparent authority is established, the agent's act nevertheless was of a character that prohibits reasonable reliance. Under a corollary "escape valve" rule, principals may avoid tort liability for an agent's acts when the agent's acts fall outside the scope of employment or scope of duties (i.e. see detour and frolic doctrines).

A rule that calls for a user to be "bound" by the operations of an electronic agent fails to take account of the types of situations for which the exceptions carved out in contract, tort and agency law have been developed. Simply holding that the operations of an agent are to be deemed the acts of a user leaves room for underlying fairness and exculpation rules to operate. It may be appropriate to note the availability of these types of defenses in commentary to the statute.

The Working Group also expressed concern about the potentially confusing terms "configures or enables," which could be read to apply to the person that installs the agent rather than the user. The word "uses" was suggested by the Working Group rather than "configures and enables" an electronic agent. The current draft UETA speaks to one who "used" an electronic agent.

Some members of the Working Group favored indexing attribution of an electronic agent's operations only to a person who engaged in use of the electronic agent for that purpose. The concern raised was that complex implementations may be capable of acts or operations that are non-obvious or unpredictable by a user and which the user should not be committed. Situations constituting intervening/superceding causes, product malfunctions and unreasonable reliance by another party were discussed. Some members of the Working Group, however, disagree with an intent test such as seems to be embodied in the current draft's use of the rule: "Operations of an electronic agent are the acts of a person if the person used the electronic agent for such purposes" (emphasis added). Those members take the view that, where an innocent party experienced some loss , the counterparty should not have as a defense that her electronic agent acted against her purposes. If she made the choice to use the agent, she should assume responsibility for its acts, again subject to available defenses such as reasonable reliance. These members would likely prefer wording proposed by the Working Group at the Atlanta meeting (see above):

The first clause of the Working Group's tentative language (above) is intended to make it clear that no formalistic legal barrier exists to persons wishing to use electronic agents. The second, more substantive clause is a simple rule of attribution deeming the acts of the agent to be the acts of the user. The understanding underlying this approach is that the legal consequences that would flow from those acts would and should be subject to defenses of the type described above. Inclusion of the word "resulting" was intended to link the actions which in fact set the electronic agent in motion with the consequent operations of that agent. In other words, an agent that is in fact hijacked by another person (or agent) and which then followed

that inter-meddler's bidding may not be the result of the original User's activities. This would be an objective determination, however, instead of the more subjective determination of the user's purposes.

5. Possible Need for Different Rules For "Instruction Bound" vs. "Autonomous Intelligent" Electronic Agents

Another concept not discussed by the group in Atlanta but considered by the co-chairs is that a "one size fits all" rule for electronic agents may not be workable. Current applications of electronic agent technology tend to be fairly limited by their algorithms and do not attempt to "learn" or predict their user's desires. For example, an Amazon.com program that leads a user through the selection process and completes the sale of a book or CD, and most automated inventory management systems, do not negotiate prices. Agent technology already in existence and starting to be deployed, however, is capable of more complex "autonomous" decision making skills and, particularly when interacting with a community of other agents, so-called "emergent behavior" can result. Emergent behaviors cannot be predicted based solely on an understanding of the constituent parts of the system. In such a case, particularly as between several users of agents who each voluntarily set their agent in motion in a community of agents, it may not be appropriate to hold a user responsible for emergent behavior of its agent. This suggests that a different rule of attribution (and perhaps substantive liability rules as well) may need to be developed to address the unique and complicated results of emergent behavior of artificially "intelligent" mechanisms. Especially in systems designed to accommodate multi-agent transactional environments, group emergent behavior may require development of legal rules that are specially tailored to those contexts and circumstances. Whatever concepts and wording are chosen as the applicable attribution rule for electronic agents, it would be appropriate to clarify in commentary that the statute does not address the topic of the liability of agent developers for defective design and "manufacture" of the agent, and is not intended either to expand or contract the scope of such liability, if any.

The Working Group is very much in the preliminary stages of its analysis, and welcomes any input and further dialogue on these topics.

© 1999 American Bar Association. All rights reserved.

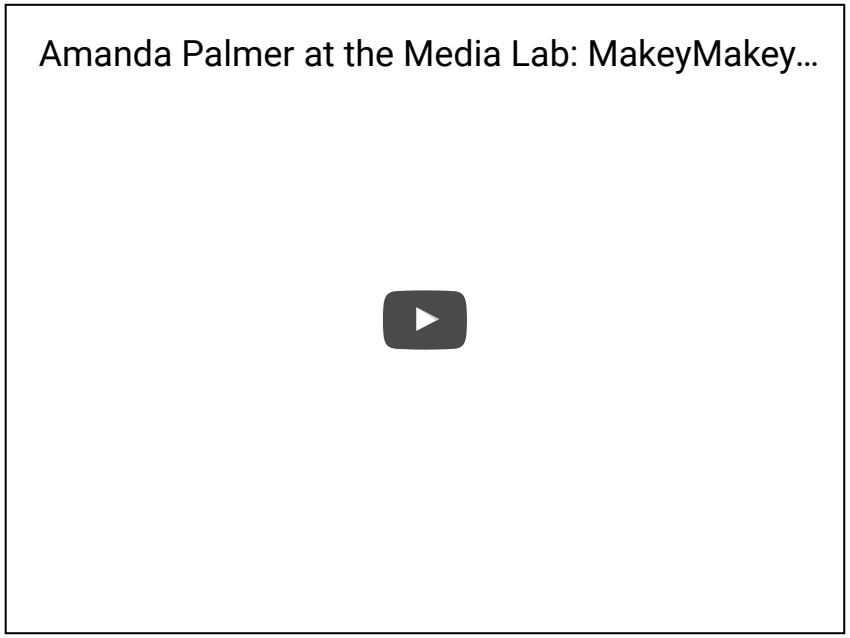
1. This draft reflects only the views of those individuals listed above. Until and unless finalization and approval of this draft occurs, neither the contents of the report, nor the opinions expressed therein, necessarily represent the views of the American Bar Association or any part thereof. This draft is a work in progress, and it is expected that final work product will be in the form of a report.

2. The revisions relate to the new definition and provisions relating to Electronic Agents in the January 29, 1999 draft of the UETA. Although the document reflects points raised in the course of discussions in Atlanta, it is still very much a work in progress. Members of the Working Group on Electronic Contracting have not yet given the Chairs their comments on this draft. There is a possibility that members of the Working Group or Committee will have further thoughts on this draft. These will be conveyed by either the members themselves or the Chairs on their behalf at that Drafting Committee meeting.

Amanda Palmer at the MIT Media Lab

Dazza Greenwood · May 30, 2012

On Monday, May 28th 2012, Amanda Palmer teamed up with the MIT Media Lab for a live webcast. The event highlighted some new and old songs, q&a with her online audience and announcements about her very successful Kickstarter campaign. The afternoon was Emcee'd and produced by yours truly, Dazza Greenwood, and it featured several demos by Media Lab grad students of projects involving music and sound. In addition to webcasting on Ustream, I also recorded some of the event with an iPad2 using an iRig Mic (for slightly better sound). Below are a couple of clips from the good old iPad2, and I'll be uploading clips of several more songs and demos and antics shortly.



Amanda Palmer at the MIT Media Lab

Update: Here's a blog nice post by "One Giant Leap of Awesome" with more links and background.

10: Identity Bill of Rights

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line 10 Identity Bill of Rights (3:15)

9: Health and Wellness

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 9: Health and Wellness (5:05)

8: Mass Customization

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 8: Mass Customization (6:35)

7: eGovernment

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 7: eGovernment (4:37)

6: Authentication

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 6: Authentication (2:58)

5: Identity Federation

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 5: Identity Federation (3:59)

4: Anonymity

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 4: Anonymity (4:54)

3: IDENTITY CONVERGENCE

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 3: IDENTITY CONVERGENCE (3:28)

2: Core Identity

Dazza Greenwood · August 22, 2010

Direct to YouTube: Your Online Identity - on The Line - 2: Core Identity (3:09)

Additional Material: special segment on Core Identity and the Core Identity Map, featuring Mark Dixon (then of SUN Microsystems) and Bob Blakely, of the Burton Group.

1: Introduction - Your Online Identity: On The Line

Dazza Greenwood · August 22, 2010

Your Online Identity: On The Line - 1: Introduction (2:29)

2.b. Core Identity Vantage Points: Mark Dixon and Bob Blakley

Dazza Greenwood · August 19, 2010

CORE IDENTITY:

CIVICS.com Focus on Identity, Mark Dixon, Bob Blakley: v.0.1 (9:46)

4.b The Privacy Club With Richard Stallman: Anonymity and Privacy:

Dazza Greenwood · November 19, 2009

The Full Privacy View

The Privacy Club: Richard Stallman Interview (9:58)

Republished 2015, Dazza Greenwood