

Application of an Autonomous Intelligent Cyber Entity as a Veiled Identity Agent

Eran Kahana

Fellow, Stanford University Law School, Stanford Center for Computers & Law (CodeX)
101 Shasta Circle West
Chanhassen MN 55317
ekahana@stanford.edu

Abstract

This position paper is based on the CodeX “Autonomous Intelligent Cyber Entity” (AiCE) book project. The AiCE draws on its intelligent and computational law capabilities to promote a safer, more efficient on-line environment. It is a flexible framework that can be configured to serve various purposes in business and individual-user settings. Due to its autonomous, intelligent and broad range functional capabilities, the success of AiCE is dependent on its entity status being formally recognized by law. This paper describes how this status can be granted by building on the same legal principles that endow U.S. corporations with an “entity” status; and while the focus here is purposefully narrowed to U.S. law, the same principles have universal application (a subject dealt with comprehensively in the book). Where the particular intention is to better protect a user’s private data, the AiCE can be configured by a user into an “AiCE Veiled Identity Agent” (AVIA). This AiCE configuration shields the user’s private information and offers him a “veiled” identity similar to that which corporate shareholders enjoy, all without degrading the flow of information vital to innovation and new value generation. This paper concludes with the introduction of the Uniform AiCE Transactions Act (UATA), an intelligent legal framework designed to govern all AiCE activity, promote trust and widespread adoption of this model.

Protecting Privacy: Anonymity & Veiled Identity

Private businesses are the prime suspects (and in varying degrees frequently guilty) of a wide variety of privacy abuse that spans from the relatively mild negligence variety to the willful, potentially criminal, type.

Attempts to protect private data sometimes appear feeble, hopelessly lagging behind the incessant exploitation. They also fail to yield adequate, predictable and sustainable remedies for victims and other stakeholders.

Copyright © 2009, Eran Kahana. All rights reserved.

Yearning for a quick fix is understandable, but there is no such adequate solution. By way of illustration, consider the attitude (attributed to Scott McNealy, Sun Microsystems’ CEO) that “there is no privacy, get over it.” While arguably seductive from the perspective that it looks like a quick and simple remedy to many complex privacy questions, it is an unacceptable position. It is an attitude that is in equal parts myopic, impractical, psychologically unsatisfying, economically unsound and altogether unnecessary.

A better privacy protection mechanism is required and this section sets the stage for how this can be accomplished. It begins with a brief review of anonymity and segues into the introduction of a new privacy protection mechanism, one that comes in the form of an identity shield known as “veiled identity.”

Anonymity

Anonymity is a venerable, but insufficiently effective identity shield. The problem? Among other things, its negative, narcotic-like side effect.

Take for example, the use of a pseudonym (an anonymity subset, per Professor David G. Post). It can occasionally embolden on-line users to behave in a manner they would not otherwise dare to; intoxicated by the assumption that their real identity (and by extension, personal/private information) is forever safely hidden, unassailable.

At a minimum, such behavior can result in submittal of less-than-useful identity-type data, amounting to a mild annoyance. But in other instances we witness anonymity/pseudonymity as negative catalysts, promoting, for example, the submission of fraudulent identity-related data that can cause significant harm to the recipient and other stakeholders.

Veiled Identity

From the instructive limitations of anonymity it is possible to move forward and construct a more efficient privacy protection mechanism, one that I call a “veiled identity.”

“Veiled identity” borrows its name from the corporate “veil” metaphor, which symbolizes the legally-sanctioned separation of the shareholder from his corporate entity. True to its symbolism, it functions as a buffer, protecting the user’s real, off-line identity, and consequently his private data, from that which is projected into the on-line world.

The veiled identity is conceptually linked to the pseudonym, but it takes that concept further and refines it. Unlike the latter, veiled identity is a legally-sanctioned construct that does not suffer from the pseudonym’s flaws, such as inability to (except in extraordinary circumstances) bring legal action under it.

It also does not suffer from the pseudonym’s intoxicating qualities. The process that the Uniform AiCE Transactions Act (UATA) requires of the user, prior to granting him the veiled identity structure, delivers a deliberate, sobering effect: Relatively to the anonymity/pseudonym model, this process substantially diminishes the probability that the user will be emboldened into believing his real identity is unassailable and concomitantly dilutes irresponsible, harmful behavior.

AiCE & the AVIA : The Entity Paradigm, Features & Benefits

Prior to describing how the veiled identity model is implemented in an intelligent, computational-law capable on-line intermediary, it is first necessary to briefly cover the corporate entity paradigm. This sets the stage for how to apply the entity concept to the autonomous intelligent cyber entity (AiCE) and its identity protection-centric configuration: The AiCE Veiled Identity Agent (AVIA).

The Corporate Entity Paradigm

A corporate entity’s person-like status is firmly entrenched in over two and half centuries of U.S. jurisprudence.

It is regularly associated with having goals, needs, welfare and enjoys protections against unreasonable search and seizure.

This entity construct can survive a disaster or die; consent to enter into contracts and breach them; commit torts, be sued, and sue in its own right for negligence, breach of contract and numerous other causes of action. The corporation also enjoys a freedom of speech, the right to property and other person-like rights.

None of this is by accident. This entity status was artificially created and intentionally conferred by operation of law for the purpose of social and economical expedience. It was done because of the (in retrospect, correct) belief that shielding shareholders from direct liability for the corporation’s actions was necessary for enabling and sustaining economic progress.

Applying the Corporate Entity Paradigm to AiCE

Using the same normative and utilitarian framework that gave rise to corporate entities, I propose a new, legally-sanctioned entity; one that is software-based and is programmatically sophisticated so as to earn the “autonomous” and “intelligent” labels.

These labels indicate the new entity has independent decision-making and computational law capabilities that can perform numerous functions. Consequently, it is able to evaluate a broad range of relevant laws; enter into contracts; evaluate legal and other website metadata; monitor and report on an on-line business’ activities to the relevant parties.

Unlike its traditional corporate counterpart, AiCE does not require all of the human-like attributes mentioned earlier. It does, however, require certain legally-sanctioned capabilities and rights in order to effectively perform its configured functions. These include, the legal right to enter into contracts; sue and be sued; and be protected from unreasonable search and seizure.

The AiCE Veiled Identity Agent (AVIA)

The AVIA is an intelligent, computational-law capable, on-line intermediary that shields the user’s real-world identity (any by extension his private data) from the on-line environment, without the negative qualities of anonymity.

It is beyond the scope and purpose of this paper to delve into the technical details of how to design an AiCE/AVIA. Suffice it to note here that these entities can be built using similar technical capabilities, such as those used by SRI International’s design of the Cognitive Assistant that Learns and Organizes (CALO), its sub-projects, such as the Personalized Time Manager agent (PTIME), or Oak Ridge Laboratory’s “Ubiquitous Network Transient Autonomous Mission Entities.”

Forming an AVIA

Forming an AVIA bears certain similarities to forming a traditional corporation. When electing to use an AVIA, it is necessary for the user to provide certain identifying, personal information for inclusion in the AVIA’s metadata, and UATA specifies which information is mandatory, and which is optional.

The AVIA user’s identifying information is split into 2 data levels: One public, the other private.

The on-line (non-personally identifiable) data is referred to as “Level A.” It endows the AVIA with data that it will use in its various on-line interactions and contains, for example, the AVIA’s name and address (IP-type) for AiCE-based service of process and other needs. Additionally, although this is still under consideration, is the idea of including certain encrypted financial information into this level. This would allow the AVIA to enter into transactions that require payment.

The second, “Level B,” is comprised of user-identifying data intended for off-line use. It requires, for example, the

(human) party designated to receive service of process, and taxpayer identification. This level may also contain financial information and it is possible that the financial information being considered for Level A would tie in with it for the purpose of payment validation and other needs.

Setting acceptable levels of risk is also part of the AVIA formation process. Here the user is tasked with selecting the on-line business categories the AVIA is allowed to interact with. For example, the user may decide the AVIA is prohibited from accessing pornographic websites, those that advocate hate and any other type of site the user finds objectionable. Similarly, the user can dictate that the AVIA seek out sites that promote social tolerance and any other information and service categories the user wants to be associated with, albeit in a veiled-identity capacity.

Intelligent Environment

Enabling optimal interaction between the AVIA and the website's legal metadata (LM) is critical for transactional efficiency. For this reason, UATA sets minimal web-design standards and on-line businesses who choose to participate (while such participation remains optional) must adopt them.

Implementing such design standards is beneficial for all stakeholders. It creates an intelligent, on-line environment and sets the stage for AiCE oversight of the website's entire scope of LM, which is comprised of representations, warranties, terms, conditions and the privacy policy.

An intelligent environment also enables the AiCE to engage with the AVIA in a variety of transactions (as allowed by UATA). They can, for example, negotiate and agree on privacy terms and conditions that are different from the default, thus permitting the AVIA to transact with an on-line business it would not have otherwise agreed to engage with.

AVIA & Legal Action

The AVIA's autonomous, intelligent and computational law capabilities allow it to analyze the LM, reference UATA and other relevant law as necessary, and make decisions on whether or not to consent to transact with a particular business.

Once consent is granted, the AVIA's task of use-monitoring commences. In that capacity, it can handle multiple missions, such as identifying instances of deceptive practices and/or breach of any part of the LM by the on-line business.

The AVIA's authority to pursue legal action against a website (intelligent environment or not) is set in UATA. It is authorized only in instances that involve negligence, gross negligence or reckless conduct. Where these instances give rise to a breach of the LM, they are handled by the AVIA as a breach of contract, and remedies are dispensed in accordance with the relevant provisions of UATA.

Compliance with Fair Information Practices

The AVIA can help reduce non-compliance costs for on-line businesses and other stakeholders. For instance, it can simplify compliance with the Federal Trade Commission's (FTC) five "Fair Information Practices" (FIP): Notice, choice, access, security and enforcement.

The "notice" of LM becomes easier to effectively prove and enforce since an AVIA is unhampered by inattention, lack of understanding, insufficient opportunity to review and other limitations that typically beleaguer human users and hinder enforcement.

As to the second FIP, "choice," UATA provides that the act of using an AVIA sufficiently manifests a user's consent to accept the AVIA's decisions. Consequently, the AVIA disarms potentially complicated questions relating to whether adequate consent was given to the relevant LM.

The "access" FIP is enhanced and satisfied because the AVIA monitors what private data is stored, by which website, how, where and when it is used. As a collateral, this also serves to bolster the "security" FIP, most significantly so if the AVIA is interfacing with an AiCE, as would be the case in an intelligent environment.

Finally, as it relates to the fifth FIP, "enforcement," it bears to mention again that there are a number of legal disputes that can be independently managed by the AVIA per the provisions in UATA.

Private Enforcement Regime

A myriad of laws regulate the scope of allowable use of private information and the FTC and the courts are well versed in them. Effective enforcement, nevertheless, remains a challenge to be satisfactorily addressed because these governmental institutions lack sufficient resources to do so.

So long as it does not run afoul of the law, a *laissez faire* approach of utilizing an intelligent, private enforcement mechanism can present an attractive, alternate regime for addressing the gaps traditional legal institutions are unable to fill.

An AVIA fits in perfectly. It easily adapts as a mission-critical tool in this intelligent private enforcement framework. It efficiently resolves many (if not virtually all) of the current disputes that arise from a user's lack of understanding, notice, and opportunity to negotiate LM terms, and correspondingly unburdens the legal system from having to deal with them.

Adjustable LM

A number of factors drive the desirability for a business to make frequent adjustments to its LM. These include a fluid state of relevant law, insurance requirements and keeping up with industry-relevant best practices.

Using an intelligent environment and a tandem AiCE-AVIA configuration is the optimal configuration for enabling this.

The presence of the AiCE allows the on-line business to easily and as frequently as necessary adjust its LM. The

presence of the AVIA, on the other hand, disposes of human-centric complications due to, for example, inadequate notice, which can militate against LM enforcement, especially in business to consumer settings.

User Profiling and Other Ills

In non-AVIA settings, a user's disclosure of his private information is not limited to intentional disclosure. Inadvertent disclosure can occur from a user's surfing habits.

While some Internet users knowingly permit tracking tools (such as cookies) to reside on their computers, there is alarming evidence that stealth use-monitoring tools proliferate. And even where some users know about these monitoring tools, there is no assurance that they can disable them or efficiently monitor how their surfing habits and other private data is or will be used going forward.

These difficulties can be resolved by the AVIA's monitoring of what data is sent from a user's computer. Such activity can take the form of filtering the information and dynamically reformatting certain parts of it to the veiled-identity structure, relieving the user from any threats associated with Level B-type data being spread into the Internet.

Legal Framework: Uniform AiCE Transactions Act

Legal sanction, coupled with effective jurisprudence to manage corporate transactions remains the critical mix for fostering trust and widespread adoption of the corporate entity model. The same principle holds true for the AiCE and any configuration, such as the AVIA.

This section highlights a select number of features related to the legal framework proposed by this research project, beginning with a review of UATA and concluding with a brief look at its drafting and placement in the legal system.

Structure and Scope

UATA is a novel, intelligent, computational law framework designed to govern all types of AiCE activity. It is also the legal framework which endows AiCE with the legally-sanctioned, corporate-like entity status mentioned earlier and formalizes the veiled identity model.

Part of UATA is an amalgam of various established legal doctrine. As such, it borrows (as necessary) from a wide variety of legal resources including uniform laws, with a significant influence from the Uniform Electronic Transactions Act (UETA), the Uniform Computer Information Transactions Act (UCITA) and the Uniform Commercial Code (UCC), specifically Article 2 (which governs sales of goods).

UATA also borrows from legal "principle" publications, most prominently from the American Law Institute's Principles of the Law of Software Contracts (PLSC).

Other influencers include the Model Business Corporations Act (MBCA) and the Internal Revenue Code (IRC).

UATA prescribes how to form an AiCE and depending on the chosen configuration, what data is required of the human user and the range of permitted functions an AiCE, in any of its numerous configurations, may perform.

UATA also instructs as to the parameters where an AiCE can take legal action against a traditional on-line business or another AiCE; identifies the venue for such legal actions and provides the available remedies for a wide range of actions.

UATA addresses a myriad of on-line contracting issues, and devotes detailed attention to aspects relating to contract formation. Here it looks at, for example, the opportunity to review, notice and consent in the context of AiCE transactions with on-line businesses and other AiCE.

Since an intelligent environment represents the optimal transaction setting for the AiCE, UATA also sets out the rules for designing such an environment. And to ensure its own optimal interoperability with AiCE and other intelligent environments containing, for example, statutes, common law, and administrative regulations, UATA is set in an intelligent environment and is itself managed by an AiCE.

This AiCE's task is to monitor UATA's efficacy and it is authorized to suggest (but not execute) amendments to UATA as well as recommend what other relevant rules and laws should be reformatted into an intelligent environment. The AiCE's recommendations are delivered to the body in charge of administering UATA (one candidate under consideration is the FTC).

Legal Action

Whether it be to counter user abuse of the AVIA model or to undertake legal action for breach of contract, UATA recognizes that legal action will need to be taken at some point.

Piercing the Entity Veil. AiCE and AVIA's veiled identity feature is not immune from user-based abuse. For example, it is possible that a user would setup an AVIA for an illegal purpose. To counter such instances, UATA provides a veil-piercing mechanism similar in principle to that used in traditional corporate settings, permitting legal action to be initiated directly against the human user.

Civil and Criminal Legal Action. The AVIA can initiate a civil lawsuit against an AiCE (and vice versa) or an on-line business, alleging, for example, a breach of contract for negligently managing private data. It is also permitted to initiate proceedings that seek injunctive relief either against an on-line business or another AiCE.

In contrast, where criminal activity is concerned, traditional legal mechanisms will be required to intervene. AVIA, however, can play a vital role in alerting law enforcement to potentially criminal malfeasance, such as unauthorized interception of electronic communications or identity theft.

Drafting and Placement

Formal drafting and delivering UATA to the point where it can fulfill its intended function will require the effort of a cross-functional team. Ideally, this group will be comprised of academics in the area of computer science and the law, lawyers, and representatives from the high-tech business community.

Where UATA will ultimately sit in the legal system, is a work-in-progress. One option currently being considered places UATA in a federal legal framework, modifiable only by Congress, and with primary enforcement responsibility resting with the FTC.

References

Post, G., David. *Pooling Intellectual Capital: Thoughts on Anonymity, Pseudonymity and Limited Liability in Cyberspace*. 1996 U.Chi. Legal F. 139.

Shane, A., Sanford. *The Corporation is a Person: The Language of Legal Fiction*. 61 Tul. L. Rev. 563 (1986-1987).

Berry, Pauline, et al, *Deploying a Personalized Time Management Agent*. Artificial Intelligence Center, SRI International.

Cody, P., Jonathan. *Protecting Privacy Over the Internet: Has the Time Come to Abandon Self-Regulation?* 48 Cath. U. L. Rev. 1183 (Summer 1999).

Hetcher, Steven. *The FTC as Internet Privacy Norm Entrepreneur*. 53 Vand. L. Rev. 2041 (November 2000).

67A C.J.S. Parties § 170, Assumed Name.

Lemley, A., Mark. *Terms of Use*, 91 Minn. L. Rev. 459 (1996).