# A social contract for cyberspace

Dawood Sheniar
*Faculty of HES*
*University of Southern Queensland*
dawoodsallemhussian.sheniar@usq.edu.au

James Northway
*Faculty of HES*
*University of Southern Queensland*
James.Northway@usq.edu.au

James Talbot
*Faculty of HES*
*University of Southern Queensland*
James.Talbot@usq.edu.au

David Millsom
*San Andreas Technology USA*
millsom@aerie.sanandreas.com

Yan Li
*Faculty of HES*
*University of Southern Queensland*
yan.li@usq.edu.au

Ron Addie
*Faculty of HES*
*University of Southern Queensland*
ron.addie@usq.edu.au

***Abstract*—The current standards for the Internet and its services and devices are set and developed by multiple standards organisations, and national governments. In this paper, we argue that a *social contract* is needed between these organisations, and the entities (individual users, organisations, devices, and service providers) which use the Internet to communicate. Criteria which a social contract should meet are proposed; fourteen major current cybersecurity or ethical issues are then discussed; the necessity and feasibility of a social contract are considered. A draft social contract is then proposed and solutions or strategies to address the fourteen issues identified previously, on the basis of this draft social contract, are presented.**

## I. Introduction

As the Internet and its residents, human and otherwise, grow in expressiveness, creativity, and energy, it seems inevitable that there will also emerge a growing need for, and development of, *regulation*. To some, this may seem like a betrayal of the original ideals of the Internet. On the other hand, if such regulation is neglected, as we argue it has been up to now, the regulations imposed by nation states, corporations, and other stakeholders, might cast an unnecessary and unwanted shadow on cyberspace. In this paper, we argue that cyberspace needs a *social contract*, with its entities (individual users, organisations, devices, and service providers), and we go on to set out criteria for such a social contract, we review the issues which it addresses, we propose a draft contract, and, finally, we review how well this draft contract addresses those issues.

The main contribution of this paper is to demonstrate the need for a social contract for cyberspace (and the Internet), i.e. a declaration of responsibilities and rights of all members of cyberspace, and also to propose a draft of such a social contract.

Any such social contract will need to enable and manage the conditions for safety and security, rather than enforce them. Details of protocols, services, and protections will still need to be the responsibility of entities that participate and contribute to cyberspace. The task before us is not to design such safeguards and mechanisms, but rather to enable their free and effective development, evolution, and deployment.

In the remainder of this introductory section, we review the initiatives in the recent history of cyberspace which overlap most closely with the work of the present paper and then outline the rest of the paper.

### A. The Social Contract

The concept of a social contract appears to have originated in ancient Greece, with the sophist philosophers and Epicurus. Plato has been found to both explain the concept of the social contract and to reject it (as a foundation for justice) [13] . The Magna Carta was a legal agreement by the English King John guaranteeing certain rights and protections to the English barons, declared in 1215, and revised and redeclared multiple times since then. Although originally it protected only barons, its extension to all free men and women appears to have been perceived as a logical necessity in subsequent years.

According to Hobbes [5], without a social contract, life is subject to

> *continual fear, and danger of violent death; and the life of man, solitary, poor, nasty, brutish, and short.*

However, a social contract between the citizens of a society enables them to co-operate effectively, to achieve a better life without the need for constant fear.

The Internet has made computing social [12]. In turn, the Internet and the cyberspace based on it, is susceptible to a number of social ills that may befall any society, such as constant harassment, belligerent attacks on property, that is, cyberattacks, and invasions of privacy which seriously compromise the benefits for our social, educational, and commercial lives. Are these issues (which are surveyed in more detail in Section III) due to the absence of a social contract?

Although the Declaration of Independence of the United States of America stated

> *We hold these truths to be self-evident, that all men are created equal, that they are endowed by their Creator with certain unalienable Rights, that among these are Life, Liberty and the pursuit of Happiness,*

slavery remained a part of the society which subscribed to this social contract for another 80 years. Social contracts have been adopted in many modern nations, and in many cases they appear to provide a good foundation for civil society, providing safety, wide-ranging freedom, with a high standard of living. Attempts to formulate an *international* social contract, have been at best partially successful. There is an international court of justice, but many nations do not accept its jurisdiction [15].

### B. Service Level Agreements

Currently, users of the Internet are likely to have agreed to a *service level agreement* with their Internet provider [8]. Functionally, this is similar to a social contract, the main difference being that the roles envisaged in such agreements are quite asymmetrical – the provider has certain obligations, and so does the consumer of their services, but these obligations are usually quite different. This is discussed in more detail in §IV-B.

### C. Standards

The current standards for the Internet and its services and devices are set and developed by multiple standards organisations [7] and also national governments. In this paper we argue that a *social contract* (like a constitution and a bill or rights) is needed between these organisations, and the entities which use the Internet to communicate.

### D. Web 2.0, the Semantic Web, or Web 3.0

Web 2.0 [17] is a name used to explore and to some extent explain the social network applications and development that has emerged from and in turn influenced the world-wide web.

Web 3.0, or the *semantic web* [1] provides a systematic standardized technology for cross-referencing, from document to document, and to specific parts of documents. Furthermore, by this means, and by agreed conventions for how key information is stored, the agents which operate in user and network devices are able to extract not just data but also the *meaning* of this data from the documents they have access to. This is achieved, it is claimed, by using XML to structure data, and RDF [19] to describe its meaning. In this way, the quality and effectiveness of the services provided by the Internet will be transformed, according to the proponents of the Semantic Web.

### E. The dark side

Some of the developments anticipated in the semantic web concept have come to pass. However, the problems listed below, in Section III, undermine somewhat the idea that facilitating reference, access, and meaningful interpretation of web data, will enable good sense to triumph in cyberspace. With the convenience and intelligence offered by electronic agents inhabiting the web, and the world of apps, a crowd of unwanted denizens focussed on criminality, exploitation, fraud, and chaos have taken the opportunities (of which there are many) to join us in cyberspace.

It seems that we need more than a universal API for access to the meaning in the Internet and its contents to ensure that good sense has enough advantage over greed, competitive advantage, and, in general, the forces of human frailty. We must assume that whenever there is an opportunity for error, fraud, deception, or intimidation, it will be exploited. We need to actively defend against criminality, greed, parochialism, and chaos.

### F. Outline of the paper

In Section II, criteria for a social contract for cyberspace are outlined, in Section III, fourteen serious and on-going ethical or security issues in the Internet and cyberspace are reviewed, in Section IV, the questions of whether a social contract is really necessary, whether it is possible, and also whether in a sense it already exists are explored, in Section V a draft social contract is outlined, including a review of how this draft social contract succeeds in addressing the issues presented in Section III, and, finally, in Section VI conclusions are presented.

## II. Criteria for a Social Contract

C-1. Any entity using the Internet is able to achieve its goals (including adequate cyber-security), by setting and enforcing their public policy, so long as this policy is consistent with the social contract for cyberspace

C-2. The obligations and rights *provided by the Internet social contract* are the same for all entities.

These criteria are natural and yet quite powerful, and we shall see that their implications are surprisingly effective. Because the ethical assumptions made by members of cyberspace are currently not explicit, it is not possible at present to explain these criteria by reference to existing work.

The first of these criterion merely says that all entities are entitled to *be able* to engage securely with the Internet, so long as they do not seek to transgress its norms.

The second criterion is the natural condition that any rules should apply uniformly to all participants. Note that the specific policies adopted by, and agreed to, by entities in the course of providing and using services are not expected to be the same for everyone.

## III. Current Ethical and Cybersecurity Issues

Cyberspace is currently burdened by many chronic and serious issues which frequently cause harm. Here follows a classified survey of such issues, including some account of their particular features in a form which is relevant to their subsequent discussion, in §V-D.

### A. Cyber-Attack

*Issue I-1. Cyber-warfare:* Most developed nations currently posess a national agency engaged in defence, *and attack*, through the Internet, against the cyberspace services and resources of rival nations. These agencies seek to gain access and defend against access by others to public and secret information about technology (especially military technology), politics and commerce. Such agencies also frequently engage in *disruption* of the same systems. Probably the most famous example of such activity is the development and deployment of the *Stuxnet* virus (actually called the *Olympic Games virus* by its developers) [10], [**?**] .

Stuxnet is a very sophisticated malware program designed to attack industrial cyber-physical systems [9]. It targetted a specific industrial laboratory – the Natanz uranium enrichment plant [9]. The challenge was that this plant is completely isolated from the Internet [2]. Stuxnet is designed to be autonomous [10]. It used four zero day exploits [2], which made it difficult to detect or prevent using the security technologies available at the time.

The development and deployment of Stuxnet has been noted as a major backward step in the standard of behaviour that might be expected in cyberspace. Any agreement, technology, or architecture that is able to prevent recurrences of this behaviour will be universally applauded, but it is unlikely that any nation will adopt measures which do that unless they can be *certain* that these measures apply to *all* entities equally.

Cyberwarfare is the most critical of all the issues we consider, and also has the greatest natural association with the question of regulating good behaviour. If a social contract can help us with this issue, it deserves our strong support.

*Issue I-2. Viruses:* A virus is an item of software that installs itself, or is installed (usually without the conscious knowledge of the user), and then runs on a user's computer, or device, or on a server, and takes actions unwanted by the user, such as stealing, corrupting, or encyrpting data.

Viruses are developed by state actors, such as the agencies referred to in I-1, by criminal organisations, working to generate income by extortion or fraud, and by individuals.

*Issue I-3. Identity Theft:* The simplest form of identity theft is for an attacker to find, discover, or guess another user's password, and then use it for services they are not entitled to.

The more complex form of identity theft is where an attacker gathers information about a target person, mostly or all from public sites, and then uses this information to take control of resources (bank accounts, phone accounts, etc) of the victim.

*Issue I-4. Fraud:* A simple example of fraud which is currently feasible in cyberspace is the unintended release to, or alteration by, a third party, of credit card or financial account credentials. For example, the account into which an employee's salary is to be paid.

*Issue I-5. Phishing:* Phishing is the practice of tricking the target into an unintended action by sending them an email (or message) which appears to be from a trusted source, or is of a frequently recieved and therefore expected form, which then triggers a semi-automatic response which has, in this instance, an unexpected (and probably secret) side-effect, such as installing a virus.

### B. Exploitation

*Issue I-6. App-stores and Software Repositories:* App stores such as Apple's App Store, and the Play Store on Android smart phones play an important role in the protection of users from attack. Software provided in an App Store is checked by professional staff. In addition, all apps are required to declare a policy which is then enforced by the smart-phone operating system. This much is entirely consistent with the social contract proposed in Section V.

However, this method for distributing and validating smart phone software directly contradicts Criterion C-2. Operating system vendors are adopting a highly asymmetical role relative to users in this approach to protection of users.

*Issue I-7. The Gig-economy (Uber et al):* Along with streamlining and increasing flexibility, repackaging services to handle service description and payment details by means of a smart-phone app, the so-called Gig-economy, has frequently had the side-effect of disempowering many of those involved in providing the service (the workers).

*Issue I-8. Monopolistic behaviour:* Monopolistic behaviour in the information, communication and computer industry has been prevalent virtually from the start. It has been addressed, in the telecommunications industry, by anti-trust legislation in the United States and similar legislative changes were adopted afterwards in many other countries. This intervention of the legal and legislative arms, of the U.S. and other governments, was viewed by many, at the time, as unwarranted meddling. However, with the perspective provided by 40 years of history, it appears to have been justified, and highly successful.

It was, nevertheless, highly disruptive, and if there are means to avoid the necessity for intervention by politicians and judges, it will be preferable.

### C. Social networking

*Issue I-9. Exile or censorship (of social network users):* The policy of banning certain users from access to Facebook,

twitter, or another social media application because of their perceived promulgation of false or dangerous beliefs is likely to be contentious [12]. Whether certain beliefs are false, or dangerous, is unlikely to be ascertained with universal agreement by any board of review no matter how carefully chosen.

*Issue I-10. Fake news:* Fake news is the name given to false information promoted as genuine, either in error, or knowingly because the promoter wishes other cyberspace citizens to be misinformed [**?**]. The widespread availability of digital sources of information, including digital signatures to verify authenticity, is reducing the scope for deliberate disinformation, but for the moment it remains a problem.

*Issue I-11. Cyber-bullying:* Bullying is a phenomenon of concern that goes beyond just the forms appearing in cyberspace. However, social networking, and cyberspace in general, can have the effect of intensifying such bullying to unprecedented, unacceptable, levels.

*Issue I-12. Protection of minors:* Before the age of approximately 18, citizens are not regarded as competent to indendently engage in society. Up to approximately this age, they require the supervision and protection of a guardian, usually but not always a parent. For example, children below this age engaged in play or exercise in a swimming pool *must* be accompanied by a responsible adult. Society includes risks of many sorts, and so, such supervision and responsibility is required almost constantly for non-adults. Cyberspace, as a part of society which reflects most of its components (good and bad), is also a domain in which supervision and guidance is required.

*Issue I-13. Local cultural traditions (locality, community):* Cultural, social, legal, and ethical traditions vary from place to place, and from community to community. Although the sharing of a medium of exchange for services and information might be expected to introduce greater homogeneity in such traditions and conventions, it is not appropriate to empower or enable such a process of convergence. On the contrary, it seems more reasonable that local traditions, if they are genuinely supported by a community, should be enabled and preserved.

Is it feasible to define and adopt a common social contract which is also neutral in its impact on locally distinct cultural traditions?

### D. Technical Development and Evolution

*Issue I-14. Standards Evolution:* The majority of Internet standards take the form of RFCs, [8] which are developed under the supervision of the IETF [7]. These standards can be of critical importance to the technical and financial success of the companies providing hardware, software, and services supporting cyberspace, employees of whom are the main particpants in the committees which develop new standards. Consequently there is a considerable risk of conflicts of interest in the development process.

## IV. Necessity and Existence?

Is it perhaps possible to achieve the criteria for a social contract for cyberspace without any such agreement being formed? Or, on the contrary, can we show that these very reasonable objectives are unattainable without such an agreement? Is a social contract which addresses any of these issues actually feasible (see §V-D)?

Let us consider whether a social contract is possible, and if it is possible, how might it be enforced.

### A. Do the existing standards form a social contract for cyberspace?

The main Internet standards are known as RFCs (Request for Comments) [8]. There are currently more than 9000 RFCs. These documents provide detailed technical descriptions of all the main protocols and algorithms used to implement the Internet. The primary form taken by these documents is a description of how certain types of communication *must*, or in some cases, *may be* formed (some features and procedures are optional).

A scan of the RFC collection using terms with likely association with a contract for cyberspace shows that even when these terms are used it is in the context of organization or technical specification but not in the context of implementing or discussing a social contract as proposed in this paper. The search terms used in this scan of the RFCs were: `ethics`, `society`, `social`, `moral`, `morals`, `human`, `humane`, `governance`, `organization`, `contract`, `service`, `SLA`, `agreement`, `privacy`.

Standards other than RFCs, which are issued by the other standards bodies [18], [6], [3], [4] (and perhaps some other organisations) also play an important role in defining and regulating the Internet.

The funding for these standards bodies comes from governments, commercial organisations, and private individuals (for example, members of the IEEE). In most cases committees of qualified professionals are formed which meet from time to time, discussing issues and details of proposed standards, and then formulating original drafts and subsequently revisions of standards. The time required by individuals in such committees is a significant cost, which in most cases is borne by the organisation from which the individual comes.

### B. Do service level agreements form a social contract?

Existing service level agreements tend to be designed primarily to provide legal protection against complaints from customers. The widespread (almost universal) existence of service level agreements acknowledges their logical necessity. However, they are rarely written in a manner which fully respects the reciprocity of the relationship between service provider and client, and there is often no discussion of enforcement.

### C. Is a cyberspace social contract necessary?

Political social contracts *emerged* in the form of the Assize of Clarendon (1166), the Magna Carta (1215), "An Agreement of the People" (1647 – during the English civil war), the U.S. Declaration of independence (1776), and the Declaration of the Rights of Man and of the Citizen (France, 1789), and, finally, the United Nations declared the *Universal Declaration of Human Rights* in 1948 [11] with 48 of the 58 nations voting for it. The difference between an "emerging" social contract, and one which is explicit, and enforcable is important. Conscious awareness of enforcability will enhance its effectiveness. Just as, in many societies, a social contract has been found to be beneficial for the prosperity and well-being of citizens, a social contract can enable the prosperity and well-being of the entities which inhabit cyberspace.

### D. Is a social contract possible?

The usefulness of the type of social contract considered in this paper depends to a significant degree on its enforcability. We shall see, in §V-D in the case of Issue I-7, that some policies are readily and naturally enforcible. Enforcibility also appears to be feasible for many other policies, e.g. I-4. Before it can be implemented as a standard, it will be necessary for the community of Internet practitioners, academics, and users to debate the matter. If there is sufficient support, progression to a standard would then proceed according to the usual process for RFCs.

### E. Enforcement

Traditionally, the legal framework of a nation state, which is the main substance, in mass, of the social contract adopted therein, is enforced by a legal system of police, courts, lawyers, judges and juries. This system is empowered to impose imprisonment, exile (in the case of non-citizens), and fines.

In the case of cyberspace such remedies are rare, but not unknown. Imprisonment is highly unlikely to be used as a remedy [12], but exile (in the sense of preventing access to certain services) has become a preferred remedy in some contexts (for example, President Trump's exile from twitter).

A more universally applicable enforcement mechanism, however, is probably the maintenance of public, incontrovertible records of past actions. The most prominent example of this currently is the block-chain system adopted in Bitcoin, and other digital currencies. Block-chains that provide public incontrovertible records of actions have also been adopted for other purposes, for example records of share transactions.

A public, accurate, incontrovertible record of actions serves more or less directly as an enforcement mechanism in the case of the social contract proposed in Section V because each entity which provides services is required to provide a *public policy*. This public policy is not merely a collection of words, sentences, and paragraphs, which users acknowledge, but is required to be formally precise, as explained in §V-B. Consequently, whenever an entity takes an action which is not consistent with their policy, if there is a sufficiently detailed record of actions, which is public, any actions taken which are not rigorously in accordance with the public policy will be detected. An entity which takes an action inconsistent with its public policy will therefore be identified almost immediately, and this fact will be clear to all other entities.

## V. A Proposed Social Contract

In this section we show how a social contract significantly alleviates most of the issues raised in Section IV, however, because there are so many examples (14), it has not been possible to treat any of them in depth. Having proposed *criteria* for a social contract, it seems only reasonable to propose, if only as a "straw man," a candidate set of rules, for such a contract. Even if these rules are incomplete, or insufficiently precise, they can serve as a reference point for discussion and development.

### A. A Draft Social Contract

Typically, a social contract is formulated as a set of *obligations* which, if fulfilled, guarantee that a certain set of *rights* will be valid, for each individual entity (person, process, organisation, device, or agent), participating in the contract. In this section we provide a first draft of the obligations and rights that might be included in a social contract for cyberspace.

Note: constitutional or legal obligations are traditionally enforced by legal remedies, such as fines or punishments. In cyberspace, these strategies might also be relevant, but the strategy of *prevention* (enforcing the obligations) might be feasible and therefore more attractive, more widely than in a social context.

*Obligations:*

O-1. To declare and honour a fair and reasonable policy for any service which is offered;
O-2. not to deliberately cause harm, to other cyberspace entities;
O-3. not to deliberately disseminate false information.

*Rights:*

R-1. To declare and honour a policy governing access to services;
R-2. To view public content and use public services on the Internet;
R-3. to contribute public content and offer public services on the Internet.

Of these obligations and rights, the ones with most force are O-1 and R-1. We give examples (e.g. §V-D) below of how these conditions can be used to address the issues raised in Section III. It might seem that "fair and reasonable" is a rather vague condition, in O-1. Be that as it may,

the real impact of O-1 is contained in the word "honour". Failing to ensure that a policy holds may have rather serious consequences for a service provider, especially under the circumstances outlined in §IV-E. By contrast, the right R-1 probably operates, in practice, by enforcement of the policy by the network provider.

### B. Formal policies

The policies referred to in O-1 and R-1 are not "aspirational", but are required to have a precise, formal, meaning. This can be achieved by being expressed in a language that has a translation into first-order formal logic, where the predicates come from a common vocabulary adopted by all entities.

### C. Does the draft social contract meet the criteria?

There are only two criteria listed above. Let us consider them one by one, starting with the C-2, since it is easily dealt with. Since the proposed social contract does not include, in any obligation or right, any reference to a specific entity or class of entity, it appears to meet this criterion.

In the list of *issues*, there are references, in the concept of *minor*, in Issue I-12, and in Issue I-10, and also in Issue I-13 to classes of entity, and to the concept that obligations and rights might vary depending on membership of such a class. However, these obligations and rights, which depend on class membership, are contained in the policy of one or more entities, not in the social contract itself.

How membership of such a class is determined is unclear, and requires further consideration.

Now let us consider Criterion C-1. This criterion does not claim that the social contract by itself guarantees that the aspirations of agents and entities in cyberspace are achieved, but merely that they are *achievable*, so long as they are not inconsistent with the social contract.

The cyberspace entities are able to set their own policies, and can *choose* which services they wish to engage with. To assist them in this choice, they can use the policies declared by those services.

### D. Does the draft social contract address the issues?

Here we discuss how the key issues identified in §III may be addressed by the draft cyberspace social contract.

*Issue I-1:* In some respects, cyberwarfare is similar to the struggle between users and the attackers who develop viruses, except that *state actors* (i.e. nation states), have much greater resources than criminal organisations and individual hackers. This aspect is discussed in Subsection V-D.

However, in addition, nation states have direct influence (in many cases, control) of technology manufacturers and network operators. A simple but highly effective cyberwarfare strategy is therefore available to these entities: network devices may be deployed, in parts of the Internet that they control, which behave in ways not exactly as specified in the Internet standards.

A solution for this problem is provided by O-1, from the social contract. All network devices should declare, and honor, a policy which, in effect, guarantees that the device works according to the published standard. Achieving such a guarantee will not be easy, although methods for implementing software which has been *formally verified* have been investigated for many years already, and have achieved considerable success.

*Issue I-2:* Two well-known and widely deployed strategies for defending against viruses are frequently used: (i) virus-scanning – which scans all files at the time when they are first stored on the target device; and (ii) policy-enforcement – which imposes a highly constrictive *policy* which controls all the actions which can be taken, by any software or script on a device or computer. Strategy (ii) therefore already fits the architecture proposed in the social contract. Systems like SE-Linux [16], or apparmor, which is provided with Ubuntu Linux, which implement and enforce policies for all applications on a certain host, are an instance where the social contract condition O-1 is already enforced.

*Issue I-3:* Guaranteeing that user's never reveal their credentials is not something that we can achieve on their behalf. However, it is possible to declare the objective that credentials cannot be accessed, or altered, except according to a limited range of trusted procedures. Such a policy can be enforced (as discussed in the next subsection). Access to personal information can also be better controlled, and policies which ensure this can be declared, and enforced.

*Issue I-4:* This issue can be addressed as follows, using O-1. Since the employer is offering a service (electronic payment of salary) to its employees, they are entitled to expect a rational policy to be adopted, for this service, which should include a condition such as:

> *Account information provided by employees cannot feasibly be altered or used in any way except by the employee to whom it refers.*

*Issue I-5:* Let us confine ourselves to the important case where the secret unintended side-effect prompted by the phishing attack is the installation of a script, or software. Such attacks are made much more difficult by the enforcement of a policy, adopted in some operating systems already [16], that software cannot be installed unless an enforced policy – for the software – is also installed at the same time. Furthermore, this can only occur if the policy itself is approved by the user. In effect, this is the same strategy as used in Issue I-2, which is essentially the same as required by the social contract.

*Issue I-6:* The current implementation of app stores in both i-phones and Android phones appears, as discussed when issue I-6 is described, to contradict Criterion C-2, However, does it contradict the draft social contract in Section V? In particular, is it fair and reasonable to declare,

as Apple does: (a) Apple's app store is the only installable software repository service (app store); and (b) A fixed proportion (30%) of all payments for services (purchases of apps, and purchases made within apps) must be transferred to Apple. Android phones do not preclude the installation of alternative app stores. The Google app-store also requires transfer of 30% of charges to Google, but this only applies to purchases from Google's app-store.

*Issue I-7:* Uber and other gig-economy services already use policies which are enforced, and this is actually what makes these services inherently attractive. The details of the policy which is enforced, in the case of Uber, are not necessarily perfect, but the fact that this policy is both explicitly written down, for consumption by both clients and providers, and is digitally enforced, is highly significant. The trip cancellation feature in the Uber app is an example of a policy which has been publicly declared and is enforced. Depending on who cancels a trip request, and any other aspect of the incomplete trip, the potential rider is charged for the uncompleted trip.

*Issue I-8:* Consider this example from history: the bundling of Internet Explorer with Microsoft Windows. The problem arises because, in this case, Microsoft is both the *platform host* for developers of software (which runs under MS Windows), and also a supplier of its own software products which run on this platform (and, in particular, Internet Explorer). Declaration of an accurate and fair policy by Microsoft for MS Windows would reveal this conflict of interest.

*Issue I-9:* Given that each social media site will be expected, if a cyberspace social contract has been adopted, to publish its own *policy*, it seems reasonable that the only grounds for banning access to such a site, should be that a user has contravened one or more conditions of the site's policy.

*Issue I-10:* A site which fails to declare in such a policy that all the information it provides is – to its best knowledge – correct, should not be taken seriously by an of its clients. On the other hand, a site which does make such a declaration, but doesn't honour it, will have failed to enforce its own policy.

*Issue I-11:* Protection from bullying can be achieved by adopting policies, in social media sites, which empower victims. It is unlikely that social media interraction which might possibly include bullying can be dynamically moderated by a payed reviewer. However, it is feasible that a professional moderator can take retrospective action whenever they have been alerted to the occurrence of bullying.

*Issue I-12:* Protection of the minors, and others needing guidance or protection, can be achieved by means of the right, R-1, of any user, to declare and enforce an access policy. The act of adopting this policy will, in most cases, be taken by the parent or guardian.

*Issue I-13:* Users have the right, according to R-1, to enforce access controls of their own choice. Most users are unlikely to wish to develop their own access policies, however it will be straightforward for other individuals or organizations to develop such policies with a certain community in mind, and these *pre-packaged* policies can then be adopted by individuals.

*Issue I-14:* Committees involved in the development of Internet architecture or protocols should develop, publish, and adopt a policy in accordance with their particular role, including a commitment to avoid influence from self-interested industry representatives.

## VI. Conclusion

It might appear that the proposed social contract is not a technical concept but rather, merely, an appeal to the good behaviour of citizens of cyberspace. However, the authors expect that technical means for enforcing policies will become more widespread, leading to an increasingly rigorous, and technical, role for the social contract.

Let us consider the impact of a social contract for cyberspace from the point of view of users:

1. *How would people behave differently that they do today?*
   Users, being aware of their right to privacy, and genuine, validated security, will expect all services to announce and ensure that a rational, respectful policy has been published, and is guaranteed to hold.
2. *Why would people change their behaviour?*
   Users will expect all providers of services to support this approach, and when appropriate choose services which have adopted preferable policies.
3. *How would rules be enforced?*
   In some cases, notably I-7 and I-4 enforcement mechanisms are quite natural and have been implemented. In other cases, development of enforcement mechanisms will require innovation and development.

## References


[1] Tim Berners-Lee, James Hendler, and Ora Lassila. The semantic web. *Scientific american*, 284(5):34–43, 2001.

[2] Thomas M Chen. Stuxnet, the real start of cyber warfare? *IEEE Network*, 24(6):2–3, 2010.

[3] ETSI. ETSI, 2020. https://etsi.org/.

[4] International Organization for Standardization. International organization for standardization, 2019. https://www.iso.org/home.html.

[5] Thomas Hobbes. *Leviathan (originally published in 1651)*. Penguin, 1985.

[6] IEEE. IEEE, 2020. https://www.ieee.org/.

[7] IETF. ietf.org, 2019. https://www.ietf.org/.

[8] IETF. RFC documents contain technical specifications and organizational notes for the internet. Web site, 2021. https://www.ietf.org/standards/rfcs/.

[9] Stamatis Karnouskos. Stuxnet worm impact on industrial cyber-physical system security. In *IECON 2011-37th Annual Conference of the IEEE Industrial Electronics Society*, pages 4490–4494. IEEE, 2011.

[10] David Kushner. The real story of stuxnet. *ieee Spectrum*, 3(50):48–53, 2013.

[11] United Nations. Universal declaration of human rights, 1948. https://www.un.org/en/about-us/universal-declaration-of-human-rights.

[12] Manoj Parameswaran and Andrew B Whinston. Social computing: An overview. *Communications of the association for Information Systems*, 19(1):37, 2007.

[13] Plato. *Five Dialogues*. Hackett Publishing Company, 1981.

[14] Plato. *Republic*. Hackett Publishing Company, 1992.

[15] Geoffrey Robertson. *Crimes against humanity*. Penguin, 1999.

[16] SELinux. Selinux project wiki, 2020. https://selinuxproject.org/page/Main_Page.

[17] O'Reilly Tim. What is web 2.0. *Design Patterns and Business Models for the Next Generation of Software. Consultado el*, 3, 2005.

[18] International Telecommunication Union. ITU, 2019. https://www.itu.int/en/Pages/default.aspx.

[19] W3C. Resource Description Framework (RDF), 2021. https://www.w3.org/RDF/.

[20] Wikipedia. Operation Olympic Games, 2021. https://en.wikipedia.org/wiki/Operation_Olympic_Games.