<table>
<thead>
<tr>
<th>Title</th>
<th>Author(s)</th>
<th>Summary</th>
</tr>
</thead>
<tbody>
<tr>
<td>New Book: Revolutionary War Law and Lawyers</td>
<td>Thomas J. Shaw</td>
<td>The issues that led Britain's American colonies to rebel, declare independence, and engage in a war to ensure that they could enact and try their own laws, are as relevant today as they were 245 years ago. As discussed in a new book, <em>Revolutionary War Law and Lawyers – Issues, Cases, and Characters</em>, lawyers and</td>
</tr>
<tr>
<td>Australian Government Oversight to Secure Communications</td>
<td>Adrian McCullagh</td>
<td>On the last sitting day of the 2018 Australian Federal Parliament, the Parliament passed an extensive amendment to the Telecommunications Act. The amendment is known as the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 [TAA]. The TAA is designed to increase</td>
</tr>
<tr>
<td>Human Rights, the United Nations, and Digital Technologies:</td>
<td>Timothy S. Reiniger and Stephen Mason</td>
<td>This submission is in response to the June 10, 2019 call by the United Nations Secretary-General's High-Level Panel on Digital Cooperation for assistance in determining the application of human rights principles on digital technologies. In the global network information society, it is crucially important that individuals be</td>
</tr>
<tr>
<td>Ephemeral Messaging Presents New E-Discovery Challenges</td>
<td>Alexander B. Hastings, Michael Fletcher, and Edward H. Rippey</td>
<td>Information management and e-discovery seem to present a never-ending supply of challenges as technology develops, and the need to respond to these developments is ever present as vanishing messaging applications are exploding in popularity. Not only are these technologies used to convey personal messages,</td>
</tr>
<tr>
<td><em><strong>Editor's Message</strong></em></td>
<td>Thomas J. Shaw</td>
<td>Times change, technology changes and so do the places where lawyers present and learn about the latest changes to the law. So it is with some regret but fully mindful of the inevitable march of progress, that I am announcing, after ten consecutive years of publishing the <em>Information Law Journal</em> (ILJ) each quarter,</td>
</tr>
</tbody>
</table>

© 2019 American Bar Association. All rights reserved. Editorial policy: The Information Law Journal (formerly published separately as the Information Security and Privacy News and the EDDIE Journal) provides information about current legal and technology developments in information security, privacy, cloud computing, big data, mobile computing, e-discovery, digital evidence, computer crime, cybersecurity, e-commerce, and the Internet of Things that are of professional interest to members of the ABA. Material published in the *Information Law Journal* reflects the views of the authors and does not necessarily reflect the position of the ABA, the Section of Science & Technology Law or the editor.
New Book: Revolutionary War Law and Lawyers

By Thomas J. Shaw

The issues that led Britain’s American colonies to rebel, declare independence, and engage in a war to ensure that they could enact and try their own laws, are as relevant today as they were 245 years ago. As discussed in a new book, Revolutionary War Law and Lawyers – Issues, Cases, and Characters, lawyers and the legal issues that they dealt with were at the heart of the American rebellion, in the fight for individual and collective rights, in the governing structures, diplomacy and finance of a fledgling nation, and in the military build-ups and battles. Lawyers and judges were a significant majority of the members of the Continental Congress, which acted as the legislative, executive, and sometimes judicial, branches of this new national political entity. Lawyers and judges were key members of the diplomatic corps trying to find funds and friends among the nations of Europe and North America, were part of the efforts to supply armies, ensure loyalty, and discover traitors, and served in all capacities of the U.S. military and naval forces opposing the British Army and Royal Navy.

In today’s political environment, all parties claim their own interpretations of what America stands for. To truly understand, it is best to go back to the start of American collective consciousness, to the time before the nation and the Constitution were created, to look at the legal issues that arose leading up to and during this war. One example was the multifaceted issue of the lack of representation. The citizens of the colonies complained about being subject to direct and indirect taxation without representation. Judges, customs collectors, and colonial officials were often appointed in London, not locally, far away from the American people they presided over. Imperial laws were considered to be supreme over colonial statutes and imperial control was exercised over colonial natural resources, such as the trees designated for naval ship masts. Local court decisions and jury findings could be overridden by royal prerogative and access to courts, in certain cases, may have required an American party to travel to Canada or to England. Courts could be closed for not complying with revenue laws and elected officials could be prohibited from serving. Citizens protested when excessive legal fees made access to justice impossible and when states taxed real estates in unrepresented occupied areas.

This is the third book in a trilogy (first two: WW1 and WW2), about the legal issues and personalities during wartime, for the three major global wars that America has been involved in. It discusses 200 legal issues and profiles nearly 300 lawyers and judges who addressed these issues. It sheds light upon not just the American legal jurisprudence but also that of their allies, and especially that of its military opponent, with British laws, military codes, and civilian and military trials. For two nations with a common legal heritage, this was the first truly legal war, where actions by governments and military commanders required a legal basis, and where those who failed in their roles were often to subject to commissions of inquiry or courts martial. Starting from the legal issues that led to rebellion and ending with peace, the book closes by looking at unexpected legal issues that seem to arise in all wartimes, despite the separation of a century or more and vast improvements in technology and social progress.
Thomas J. Shaw runs DPO Services from the EU, is most recently the author, in 2019, of Revolutionary War Law and Lawyers – Issues, Cases and Characters and in 2018 of DPO Handbook – Data Protection Officers under the GDPR, Second edition, the author of numerous other legal technology, privacy, and legal history books, and is the editor/founder of this publication.
End of the Road for This Periodical, the Information Law Journal

By Thomas J. Shaw

Times change, technology changes and so do the places where lawyers present and learn about the latest changes to the law. So it is with some regret but fully mindful of the inevitable march of progress, that I am announcing, after ten consecutive years of publishing the Information Law Journal (ILJ) each quarter, its closure with this issue. I founded this periodical to provide a publishing space with ZERO bureaucracy within the ABA (a very difficult proposition, even at the best of times), where lawyers and technicians could easily share their experiences, with no hassles. Being a frequent author, my desire was to give voice to others, without limitations on space or content and with little editorial restriction, requiring only a professionally written article of interest to others. So, the intention was to publish a periodical for lawyer-authors, by a lawyer-author, on topics relevant to information law in all its branches. But as time has moved on, so have the places where lawyers describe and retrieve their knowledge and expertise and the number of lawyers and technicians available and willing to share their experiences here has diminished. This recalled for me a lesson learned early in my career, that one can be most successful professionally by striving to work yourself out of your current role and move on to the next challenge that invariably awaits. So it shall be with this periodical.

In this final issue, I wanted to shine a light most intensely on the many, many authors that I have had the pleasure to get to know over the years and to be able to provide a platform for them to share their insights. It is quite some number of people, several hundreds, from all parts of the globe and all differing levels of experience and practice types. I am most proud of not only the number of authors this periodical was able to attract but also the wide diversity of this group of writers. From judges and law firm partners to new lawyers and law students, I want to thank each one of them for taking the time to share. I strongly believe in freely sharing, not hoarding, one’s expertise and I hope the Information Law Journal has been, over these last ten years, a place where people learned more about those subject areas we endeavored to cover and present. It had been a unique experience for me since I first founded this publication, and its antecedents the Information Security and Privacy News and the EDDE Journal, working with so many people whom I never met in person. Although there have been higher and lower moments, it is only the former I will take forward with me.

I will close here by listing the names and submitted photos of every one of the authors who appeared in these pages, with the issue that they appeared, starting from the very beginning, ten volume years ago. It is a long list but do look to find yourself in it, for some this will be more than one entry. I strongly wish to encourage everyone to continue sharing their experiences and expertise, in whatever medium you believe is most appropriate for information law, in the near and distant future. Hopefully a new publishing forum, using the latest technologies in shared-knowledge delivery and presentation, will arise to fill this niche, for those who desire a no-hassles, ego-free, writer-focused place to publish. Best wishes to all and thank you for contributing, reading, following, and supporting us over the years.
The following is a list of authors by volume and issue, combining the ISPN and EDDEJ for issues v1i1 to v5i3 and thereafter the ILJ.

**v1i**

Scott Blackmer

Thomas J. Shaw

Ariel Peled

Hon. John M. Facciola

Thomas J. Shaw

**v1i2**

Michael A. Aisenberg

Paul Paray

Thomas J. Shaw

David D. Cross

Emily Kuwahara

Timothy Reiniger

Jacques R. Francoeur

John Jorgensen

Steven W. Teppler

**v1i3**

Mari J. Frank
Robert Jueneman
Thomas J. Shaw
Timothy Reiniger

Richard Hansberger

Christina Zachariasen
Nick Brestoff
Steven W. Teppler

Thomas J. Shaw (describing the committee’s book and significant contributors):
  Robert Jueneman
  Michael Power
  Charlene Brownlee
  David Ries
  Tom Smedinghoff
  Maria Hofmann
  David Navetta
  Steven Roosa
  Tanya Forsheit
  E. Regan Adams
  Bradley J. Schaufenbuel
  Kathryn R. Coburn
  Yakov Ginzburg
  Robert F. Williams
Thomas J. Shaw runs DPO Services from the EU, is most recently the author, in 2019, of Revolutionary War Law and Lawyers – Issues, Cases and Characters and, in 2018, of DPO Handbook – Data Protection Officers under the GDPR, Second edition, the author of numerous other legal technology, privacy, and legal history books and articles, and is the editor/founder of this publication.
Australian Government Oversight to Secure Communications

By Adrian McCullagh

On the last sitting day of the 2018 Australian Federal Parliament, the Parliament passed an extensive amendment to the Telecommunications Act. The amendment is known as the Telecommunications and Other Legislation Amendment (Assistance and Access) Act 2018 [TAA]. The TAA is designed to increase the ability of Law Enforcement Agencies such as ASIO, the Australian Federal Police and State and Territory Law enforcement agencies (Authorised Agencies) to better monitor possible terrorist and, criminal activity in real time. The TAA focuses on encrypted communications by permitting Authorised Agencies to issue a particular notice or request to seek assistance in decrypting an otherwise encrypted message in real time.

The impact of the TAA is substantial as it exposes all organisations that either:

- develop secure communication software or devices and makes that software or those devices available to the Australian market; or

- provides a secure communications service to Australian residents even though the organisation may not have any other business operations or assets located in Australia; or

- use a secure communications service as a bureau service for their own business operations;

...to a risk of a data breach or leakage that would otherwise not exist. In general, the TAA conflicts with other regulatory obligations that require organisation to secure their corporate date or the data that relates to personal identifiable information as defined under the Privacy Act.

Australian Connection

The connection to Australia does not have to involve the incorporation of an entity in Australia. The connection could be as simple as having an Australian resident utilising a service or acquiring some security device, that is provided via a non-Australian communications facility such as a server located outside of Australia. An example of this is the use of “Whats App” or “Telegraph” by an Australian resident. The actual service is operated externally to Australia but can be accessed by residents in Australia.
Objective of TAA

The TAA is principally directed at secure or encrypted communications. In basic terms an Authorised Agency is permitted to demand changes to any software that provides as part of its functionality encrypted communications.

Not all encrypted communications will be impacted. For example, internet banking involves the transmission of encrypted communications, but the functionality of the communications is very restricted and as such would not be subject to a notice from say ASIO, which is the principal counter-intelligence agency in Australia.

The background to the TAA is the perceived impediment for Authorised Agencies to adequately monitor in real time encrypted communications that may be instigated by terrorists or other criminals in the community.

To assist Authorised Agencies, the TAA was enacted so as to force any organisation that provides a communication service or software or devices, which utilises cryptographic technology, to assist any Authorised Agency in decrypting communications or by providing some assistance that will allow the relevant Authorised Agency to read the encrypted communication in clear text in real time.

Parliamentary Review

Since its inception the TAA has been controversial with substantial backlash from the Australian Software sector. The TAA is currently being reviewed by the Parliamentary Joint Committee on Intelligence and Security. Of interest, is the submission made by the Law Council of Australia, which opined that the TAA is incompatible with the EUs GDPR (General Data Protection Rules) requirements and the Cloud Act in the USA.

The GDPR applies to any organisation that processes any personal data of an EU member state resident or citizen. This will include any tourist who is visiting Australia such as backpackers. It will also include dual citizens of Australia who are also a citizen of a member state of the EU.

If an organisation handles person identifiable information about an EU member state resident and that organisation fails to comply with the GDPR then the EU commission can impose substantial penalties upon the affected organisation (presently the penalty has an upper limit of the greater of 4% of global turnover or 20 million Euros).

Scope of TAA

The TAA provides for 3 types of documents being issued:

- Technical Assistance Request (TAR): which is not mandatory from a compliance perspective;
• Technical Assistance Notice (TAN): which is mandatory from a compliance perspective; and

• Technical Capability Notice (TCN): which is mandatory from a compliance perspective.

Both a TAR and a TAN are similar in scope with the difference being that a TAN is obligatory whereas a TAR is voluntary.

**Contractual Arrangements**

If an organisation or person does receive a voluntary TAR, then the TAA provides that the affected person/organisation can enter into a contract with the Authorised Agency. The negotiated agreement may better protect the affected person/organisation than what is offered directly by the TAA. It will also provide evidence that the affected person/organisation was simply complying with the TAR as issued by the Authorised Agency.

In a practical sense, it is doubtful that any organisation would object to a TAR as it is a simple step for the Authorised Agency to obtain a mandatory notice promptly. Hence, a negotiated contract is the best option.

**Requested Assistance**

The assistance that an Authorised Agency can request includes:

(a) removing one or more forms of electronic protection that are or were applied by, or on behalf of, the provider; or

(b) providing technical information; or

(c) installing, maintaining, testing or using software or equipment; or ...

(e) facilitating or assisting access to whichever of the following are the subject of eligible activities of the provider: ...

(vi) an electronic service;

(vii) a service that facilitates, or is ancillary or incidental to, the provision of an electronic service;

(viii) software used, for use, or likely to be used, in connection with a listed carriage service;

(ix) software used, for use, or likely to be used, in connection with an electronic service;

(x) software that is capable of being installed on a computer, or other equipment, that is, or is likely to be, connected to a telecommunications network;
Secrecy of TAA

A major aspect of the TAA is that whoever is directed to provide any assistance via a TAR or TAN or TCN that person is not permitted to tell anyone even their employer. Any contravention of this secrecy obligation can result in a penalty of up to 5 years imprisonment. Consequently, an employer will not know that their software has been tampered with at the instigation of an Authorised Agency. A total loss of control over development arises.

EXAMPLE 1: If an employee of a service provider is given either a TAR, TAN or TCN (as the case may be), then that employee is not permitted to advise their respective employer. Further, the employee will be granted immunity from any civil liability because pursuant to section 317ZJ(3) any employee of a designated service provider acting in compliance with either a TAR, TAN or TCN (as the case may be) will be granted immunity. BUT this exemption will not extend to the designated service provider because it is the secret activities of the employee who is acting in compliance and not the designated service provider itself. Hence, in this example the designated service provider has no immunity, which could expose it to a substantial fine through other legislative obligations.

This obligation of secrecy includes not being able to inform other clients of the organisation that the communications service providers operations are no longer as secure as previously marketed. Consequently, the TAA has far reaching business implications.

EXAMPLE 2: the same situation as in example 1 but this time the liability extends to a contravention of the GDPR. The Australian Federal Parliament does not have the power to include any immunity that may arise from a contravention of the GDPR. Consequently, neither the employee nor the designated service provider will be able to successfully claim immunity. If the designated service provider has any assets located in an EU member state, then those assets are at risk to a penalty.

A TCN is not only obligatory but includes the added aspect that the Authorised Agency can change any communications software or change any security module that may be utilised by the service provider.

Systemic Vulnerability

The TAA further provides that any request/notice must not result in the deployment of any “systemic weakness” or “systemic vulnerability” in the target system. Hence, an Authorised Agency cannot legally request a change to the security software that would introduce a systemic weakness or systemic vulnerability.

The term “Systemic Weakness” is defined as “a weakness that affects a whole class of technology but does not include a weakness that is selectively introduced to one or more target technologies that are connected with a particular person. For this purpose, it is immaterial whether the person can be identified.” Systemic Vulnerability is defined in similar terms.
The difficulty with these terms is that there is a total lack of clarity. The use of these terms was to placate the software industry by attempting to limit the impact of a notice to only intended targets and not create a weakness that could be exploited across an entire computer system. But it is difficult to see how this can be achieved. The definition does not restrict itself to a particular person but in fact directs its focus to a selective technology which may be used by the intended target. If the requested compliance action is to amend a portion of the functionality of the software that is used by a number of clients including the target client, then that would not necessarily be classified as a systemic weakness. Hence, it is difficult to see how this definition could ever be used effectively to limit a change that does not create a risk to all persons who may utilise the service. If a change does occur, then that will inevitably create a weakness that could be taken advantage of by unauthorised third parties.

Further, it could arise that everyone involved believes that the requested change will not create a systemic weakness but either due to a lack of understanding in the change or poor implementation a systemic weakness is created.

There is nothing in the legislation that allows the service provider to reverse the change. Finally, on this point the change if made will be forever and cannot later be changed through an enhancement or new version.

**Limited right to dispute**

The TAA also provides that if a recipient of any notice or request wants to dispute the request or notice then they cannot do so through the Administrative Decisions Judicial Review Act to review the validity of the administrative decision. The recipient can only rely upon the Judiciary Act (section 39B). This is a major impediment because under the Administrative Decisions Judicial Review the recipient could dispute any facts that supported the decision whereas under the Judiciary Act only questions of law can be disputed.

**Conflicts with other obligations**

The TAA is in general in conflict with the following:

- Privacy Act; and
- Corporate asset protections.

Section 26WA describes a simplified outline of the data breach notification requirements as follow:

- An eligible data breach happens if:
(a) there is unauthorised access to, unauthorised disclosure of, or loss of, personal information held by an entity; and

(b) the access, disclosure or loss is likely to result in serious harm to any of the individuals to whom the information relates.

An entity must give a notification if:

(a) it has reasonable grounds to believe that an eligible data breach has happened; or

(b) it is directed to do so by the Commissioner.

Further, Australian Privacy Principle 11 provides that:

11--security of personal information

11.1 If an APP entity holds personal information, the entity must take such steps as are reasonable in the circumstances to protect the information:

(a) from misuse, interference and loss; and

(b) from unauthorised access, modification or disclosure.

This principle is a clear obligation placed upon a collector and holder of Personal Identifiable Information to take reasonable steps to secure such information from unauthorised access and dissemination. The obligation extends to both data at rest and data in transit.

In addition to the security obligation required for the protection of personal identifiable information, the Corporations Act (2001) Cth (Corporations Act) imposes substantial obligations upon officers of a corporation to protect corporate assets including information assets.

Section 286 of the Corporations Act provides that:

(1) A company... must keep written financial records that:

(a) correctly record and explain its transactions and financial position and performance; and

(b) would enable true and fair financial statements to be prepared and audited.

(2) The financial records must be retained for 7 years after the transactions covered by the records are completed.

(3) An offence based on subsection (1) or (2) is an offence of strict liability.
Financial records would include client information and if the corporation’s software has any secure communication functionality then the TAA could comprise that required security. Clearly from the above, there are specific information security obligations placed upon corporations and other organisation. Also, it is not unusual for software license agreements and cloud service agreement to include a provision that impose obligations that the licensed software or cloud service provider will not introduce any security vulnerabilities. Finally, software providers and cloud service providers generally market their software products and services as being secure and do not mislead or deceive the market as regards to the security of their products and services. The Australia Software Sector has promoted, as best it can, itself as being providers of trusted commercially safe services and products and has established a reputation of the highest standing both domestically and internationally. This position will be difficult to be maintained due to the impact of the TAA.

It is difficult to counteract against the impact of the TAA. This is especially so due to the secrecy provisions imposed by the legislation. But there are somethings that can be done to assist in managing the risks.

**Conclusion in Managing Risk of TAA**

The surreptitious nature of the TAA means that designated service providers are exposed to a major risk which is not of their doing.

It is recommended that:

- all privacy policies should be reviewed and at least refer to the impact of the TAA. This may assist in limiting or at least explaining a security risk/leak if it should arise;

- it may be possible to insure against the impact of the TAA though whether an insurance provider is will take up such risk is debatable.

- Software manufacturers who license their software to the Australian market may want to ensure that their software can be altered in such a way that any change can be isolated to ONLY impact a particular person; just in case they do receive a request or notice from an Authorised Agency. The relevant manufacturer could then incorporate an appropriate clause in their license to account for the impact of the TAA.

- Any organisation that provides a secure communications facility as part of their business operations may want to review those operations to ensure that their operation cannot surreptitiously be compromised.

- Any person/organisation that receives a TAR should promptly contact their legal advisor and try to negotiate an appropriate contract as provided under the TAA.
Adrian McCullagh has degrees in Computer Science and Law as well as a Ph.D. in IT Security. He obtained his Ph.D. from the Information Security Research Centre at the Queensland University of Technology.

He has been practicing in IT law for more than 30 years being one of the pioneer IT lawyers within Australia. He is a member of the Queensland Law Society and a member of the American Bar Association. In 1999 he was the QUT Faculty of Information Technology Alumnus of the year.

Even though in private practice he continues to undertake research matters with academics at the Griffith University and the University of Queensland and has published in a wide variety of academic journals in the USA, UK and Australia. Adrian was recently appointed as a research fellow at the Law Futures Centre located at Griffith University. He is a member of the Intellectual Property and Information Technology Committee for the Queensland Law Society.

Adrian’s current research interests include Telecoms security, IT security, IT governance, cryptocurrencies, Blockchain and its uses in supply chain management, Decentralised Autonomous Organisations and Identity Management. He is also investigating the impact of autonomous vehicles and its policy considerations.
Human Rights, the United Nations, and Digital Technologies: Configuring Human Rights in Software Code

By Timothy S. Reiniger and Stephen Mason

This submission is in response to the June 10, 2019 call by the United Nations Secretary-General’s High-Level Panel on Digital Cooperation for assistance in determining the application of human rights principles on digital technologies.\(^1\) In the global network information society, it is crucially important that individuals be given the juridical means to enforce their human rights in personal information. We conclude that the human rights tradition, as embodied in the United Nations Declaration of Human Rights (UDHR), is currently unrealized in the machine-space of the digital environment, which defaults to being authoritarian.\(^2\) After discussing the UDHR articles that are most pertinent, we present examples of emerging approaches that may serve as functional mechanisms for protecting and enforcing human rights in the machine-mediated age governed by software code.\(^3\)

Human Rights and Digital Technologies

To his Excellency the Honorable António Manuel de Oliveira Guterres, Secretary-General of the United Nations. (September 11, 2019.)


---

\(^1\) See “The Age of Digital Interdependence: Report of the UN Secretary-General’s High-level Panel on Digital Cooperation,” (June 2019), available at https://digitalcooperation.org/. In particular, this submission responds to recommendations 3A and 3C, found on pages 38-9 of the Report. Note that neither the Report nor this submission addresses the matter of applying the UDHR articles to the fields of human genetics and bioengineering. The authors of this submission urge the UN Secretary General to consider organizing a high-level panel to discuss this as well. For an introduction to the issues raised by software code in this context, see JEREMY RIFKIN, THE BIOTECH CENTURY: HARNESING THE GENE AND REMAKING THE WORLD(1998) (describing the application of cybernetics to processes in living organisms) and BILL McKIBBEN, ENOUGH: STAYING HUMAN IN AN ENGINEERED AGE (2003).

\(^2\) The UDHR is available at https://www.un.org/en/universal-declaration-human-rights/. The authors note that the principles of the UDHR have been incorporated in a wide variety of United Nations documents, including the International Covenant on Civil and Political Rights and the International Covenant on Economic, Social, and Cultural Rights.

\(^3\) In the context of this submission, the authors note that software code is colloquially called “artificial intelligence” and David Harel, in COMPUTERS LTD. WHAT THEY REALLY CAN’T DO 194 (2000), refers to “algorithmic intelligence.”
1. We now live in an information society or, to put it more accurately, we live in a machine-mediated age governed by software. The network communication of one item of software with another item of software governs much of what we do when interacting with machines controlled by software. Therefore, a critically important issue is the recognition and enforceability of human rights that we can expect when using machines and digital identities that are controlled by software.

2. Many individuals experience serious disruption in their lives because an identity thief has used their digital identity and additional personal identifying information and attributes contained in numerous network databases (such as government service records; bank accounts; credit bureaus; and credit card data) to secure unauthorized network access to steal from others in the name of the innocent person, creating financial losses that are difficult to resolve.

3. The reliance upon software in the information age has challenged legal systems to understand how to assess the trust placed in machines controlled by software, and how to determine and prove that a responsible person or persons may or may not be responsible for the communications between the machines.

4. Corporate and governmental surveillance of the lives of ordinary people is now ubiquitous. Yet, there is no consensus on whether informational privacy is a human right.

5. There is no consensus on whether access relations in the networked environment is a human right.

---

4 The influence of software code, network architectures, technological capabilities, system design choices, and machine-mediated environments on creating information use rules and regulating behavior in cyberspace has been referenced as ‘code is law’ in LAWRENCE LESSIG, CODE VERSION 2.0 (2008) and as ‘Lex Informatica’ by Joel R. Reidenberg in Lex Informatica: The Formulation of Information Policy Rules through Technology, 76 TEX. L. REV. 553 (1998). For purposes of this article, we give the term ‘software’ this broad meaning. See also, Dan L. Burk, Lex Genetica: The law and ethics of programming biological code, 4 ETHICS AND INFORMATION TECHNOLOGY 109, 112 –121 (2002), in which the application of Lex Informatica technological and system design policy approaches for regulating human behavior are applied in the context of programmable biological code.

5 A growing number of national authorities are now issuing identity credentials in digital form. Information on the current status by country is available at https://www.worldprivacyforum.org/2017/07/national-ids-around-the-world/.

6 This topic is discussed in detail in Nicholas Bohm and Stephen Mason, Identity and its verification, COMPUTER LAW & SECURITY REVIEW, Vol. 26, No. 1, 43 – 51 (2010).

7 This topic is discussed in detail in Stephen Mason and Timothy Reiniger, ‘Trust’ Between Machines? Establishing Identity Between Humans and Software Code, or whether You Know it is a Dog, and if so, which Dog? 22 COMPUTER LAW & SECURITY REVIEW, Issue 5, 135-48 (2015).


9 See Stephen Mason, The Internet and Privacy: Some Consideration, 21 COMPUTER LAW & SECURITY REVIEW, Issue 3, 68-84 (2015). Nor is there international consensus on the concept of privacy. Id. at 74.

B. Conditions for the Recognition and Enforceability of Human Rights

6. The origins of our current understanding of human rights traces to the twelfth-century recognition of humans as holders of inherent natural rights and the adaptations of these concepts to the conditions in subsequent centuries.\(^{11}\)

7. Historically, the recognition and enforceability of natural or human rights rests on three fundamental principles: a) human beings with inherent rational and moral faculties and powers, b) human beings with free will to act, and c) human beings with subjective rights or authority to act, including active claim rights.\(^{12}\)

8. Human rights historically have been shaped by responses to abuses by anonymous corporate structures including governments, religious institutions, and business corporations.\(^{13}\) Systems and automated processes, by themselves, do not command the trust of users.\(^{14}\)

9. Digital technologies by themselves do not threaten human rights. Instead, the threat comes from human beings.\(^{15}\)


\(^{12}\) Tierney, supra note 11, at 44-8, 64-9, 242-9, and 343-8. See also Brian Tierney, Historical Roots of Modern Rights: Before Locke and After, 3 AVE MARIA L. REV. 23 (2005); Brian Tierney, The Idea of Natural Rights—Origins and Persistence, 2 Northwestern J. INT'L Human Rights 4-8 (2004) and Charles J. Reid, Jr., The Canonistic Contribution to the Western Rights Tradition: An Historical Inquiry, 33 B.C.L Rev. 37 (1991). Note that modern physics now lends support to the concept of free will. Richard A. Muller, NOW: THE PHYSICS OF TIME 10 (2016) (“Despite arguments from classical philosophers, we now know that free will is compatible with physics; those who argue otherwise are making a case based on the religion of physicalism. We can influence the future using not only scientific but also nonphysics knowledge (empathy, virtue, ethics, fairness, justice) to guide the flow of entropy to bring about a strengthening of civilization or its destruction.”) With respect to juridical claim rights, see A.W. Brian Simpson, Human Rights and the End of Empire: Britain and the Genesis of the European Convention 3-4 (2001) (noting that an outstanding feature of the European Convention is that it gives individuals standing to initiate private judicial complaints.)

\(^{13}\) For a representative discussion of human rights abuses suffered by indigenous peoples in South and Central America and the Caribbean, see Bartolome de las Casas, A Short Account of the Destruction of the Indies (Penguin Books 1992) (estimating that 10-15 million indigenous persons lost their lives under great suffering, including torture).

And so blinded by ambition and driven by greed are the devils who advocate such treatment of these people that they cannot see that, when their victims come to obey under duress this foreign overlord and publicly recognize his authority over them, simply because of their fear of what will happen to them if they do not, such a recognition of suzerainty has no standing in law whatever, any such prerogative obtained by menaces from any people anywhere in the world being invalid. In practice, the only rights these perfidious crusaders have earned which can be upheld in human, divine, or natural law are the right to eternal damnation and the right to answer for the offenses and harm they have done....

Id. at 53-4. For a discussion of the Second World War origins of the UDHR, see Geoffrey Robertson, Crimes Against Humanity: The Struggle for Global Justice 26-34 (1999).

\(^{14}\) Joseph Vining, The Authoritative and The Authoritarian 25, 46 (1986). See also Vaclav Havel, Disturbing the Peace: A Conversation with Karel Hviždal 10, 195–96 (Paul Wilson trans., 1990) (discussing the cause of the global trust crisis as the... “conflict between an impersonal, anonymous, irresponsible, and uncontrollable juggernaut of power (the power of ‘mega machinery’) and the elemental and original interests of man as a concrete individual.”).
10. Digital technology development reflects the emerging needs of society as it is organized.  

11. In its current form, the UNDHR can be applied effectively to enable the recognition and enforcement of human rights in the global digital network-based environment.

II. Human Rights and Digital Technologies: The Pertinent Articles in the United Nations Declaration of Human Rights

A. Article 1

All human beings are born free and equal in dignity and rights. They are endowed with reason and conscience and should act towards one another in a spirit of brotherhood.

12. Subjective rights are those that are inherent to each person and are inseparably part of each personality. Therefore, such subjective rights exist whether or not contained in national legislation.

13. An essential basis for the recognition and enforceability of human rights in the global information society is the authentication of legal identity. Yet we lack a common global method for enabling and recognizing legal identities in the digital environment.

---

15 Norbert Wiener, The Human Use of Human Beings: Cybernetics and Society 181 (1954) (the real danger is that “...such machines, though helpless by themselves, may be used by a human being or a block of human beings to increase their control over the rest of the human race or that political leaders may attempt to control their populations by means not of machines themselves but through political techniques as narrow and indifferent to human possibility as if they had, in fact, been conceived mechanically.”). See also Aldous Huxley, Brave New World xiv (Forward) (1932) (“Indeed, unless we choose to decentralize and to use applied science, not as the end to which human beings are to be made the means, but as the means to producing a race of free individuals, we have only two alternatives to choose from: either a number of national, militarized totalitarianisms...or else one supra-national totalitarianism...”); Havel, supra note 14, at 13 (“The most important thing is that man should be the measure of all structures, including economic structures, and not that man be made to measure for those structures.”).

16 Mark Kurlansky, Paper: Paging Through History xvii (2016) (“Technology is only a facilitator. Society changes, and that change creates new needs. That is why technology is brought in. The only way to stop the technology would be to reverse the changes in the society.”).

17 Tierney, supra note 11, at 20-30, 42-57, 64-8, and 88. “The one necessary basis for a theory of human rights is a belief in the value and dignity of human life.” Id. at 247. For an illustrative modern application, see the West German Abortion Decision, 9 The John Marshall Journal of Practice and Procedure 605, 662 (1976) (translation by Robert E. Jonas and John D. Gorby) (“Underlying the Basic Law are principles for the structuring of the state that may be understood only in light of the historical experience and the spiritual-moral confrontation with the previous system of National Socialism. In opposition to the omnipotence of the totalitarian state which claimed for itself limitless dominion over all areas of social life and which, in the prosecution of its goals of state, consideration for the life of the individual fundamentally meant nothing, the Basic Law of the Federal Republic of Germany has erected an order bound together by values which places the individual human being and his dignity at the focal point of all of its ordinances.).

18 We note there may be legal uncertainty as to whether all Articles in the UDHR are recognized as being within the body of international law. For a discussion of this legal issue, see Robertson, supra note 13,.at 80-92.

14. The network-based economy and systems each require trust in the capability to identify and authenticate individuals who seek to obtain access to networks, share information, and sign documents.

15. Both public and private sector participants in the identity ecosystem recognize that open markets for the exchange of identity information are essential to trusted online access to networks. Nevertheless, current internet identity markets are dominated by identity management systems in which users have little or no control over their data and little to no visibility as to where their data flows and how it is used.

16. The rise of the digital network-based information economy, and the cybernetic theories upon which it is based, has produced identity deficit or increased absence of the person. For law, cybernetics governance principles and computing machines have caused profound policy crises related to authentication, authenticity, and authority. Specifically, cybernetics raises important legal considerations with respect to the manner in which information and actions are linked to persons, authenticity is proven, and responsibility is determined in systems.

17. Digital technologies order systems by means of quantifying life into bits of information or amounts of entropy. But human identity needs to be approached holistically and not analytically. A holistic

ordered or even accessed via an internet connection, we increasingly use proxy data to identify who we are.

For a discussion of how the individual is disembodied in cyberspace (also understood as the ‘space’ or network in which machine-mediated communication occurs) see DOUGLAS GROOTHUIS, THE SOUL IN CYBERSPACE 37 (1997) (Machine-mediated identity is a “medium for disembodiment.”).

Currently, over one billion people in the world lack a legal identity. For information on the lack of civil birth registration in many countries, see, by way of example, https://www.unicef.org/rosa/what-we-do/child-protection/civil-registration. A major challenge has been the lack of reliable means by which to identify persons in rural areas of many developing countries. To address this, efforts are being launched in Haiti by the Episcopal Diocese of Maine (a member of the Anglican Communion) to leverage the rural presence and vital information collected by NGOs in the form of faith-based organizations.

See, e.g., Havel, supra note 14, at 195–96 (referencing “identity that is decaying, collapsing, dissipating, vanishing” in the face of “impersonal, anonymous, irresponsible” power); GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 92 (2008) (“Fundamental to any discussion about proof of digital identity is an understanding that information systems have no intrinsic way of knowing the identity of entities that participate in the systems’ reading and writing games.”); JOSEPH VINING, FROM NEWTON’S SLEEP 248 (1995) (“[T]he personal disappears in process and system.”).

Wiener supra note 15, at 15 and 27 (defining cybernetics as the study of messages to explain purposive behavior in machines and how they regulate themselves in changing environments and systems).

Id. at 17–18, 25–27 (suggesting that cybernetics reduces all activity to processes, which consist of two ingredients: information and feedback). See also PETER F. DRUCKER, THE AGE OF DISCONTINUITY: GUIDELINES TO OUR CHANGING SOCIETY 38 (1969) (“Underlying [the information industry] is a new perception: the perception of ‘systems.’”).

Wiener, supra note 15, at 21–27 (describing the use of machines and feedback systems to stabilize performance and control the entropic tendency toward disorganization in nature and society). See also VINING, supra note 21, at 37–41.

All in this view of the world and ourselves flows from the reduction of all to process and pattern, the first step in scientific thinking, and from the associated reduction of saying to doing. Everything depends upon these two assumptions, that the person or self can be collapsed into pattern and process, and that saying can be equated to doing or “behavior,” permitting observation from the outside.

Id. at 41.
strategy identifies a person by understanding his or her relationships and functions within a larger context or community. An analytical strategy identifies a person through a reductionist method of labeling constitutive attributes or parts.

18. Recognition of the person results in greater emphasis on human choice, free will, and intent.26

B. Article 6

_Everyone has the right to recognition everywhere as a person before the law._

19. With automation and artificial intelligence, the legal responsibility for the consequences of software-related failures is obscured. With respect to machines controlled by software, we do not have direct evidence of the identity of a responsible _person_ who actually controls its use.27 In this respect, the comment by Pierre de Latil that ‘The machine will never be able to tell who directs its activity’ is highly apposite.28

20. Automatons and robots have no capability for consciousness or conscious agency.29

21. Machine or system-made evidence should be neither automatically deemed more reliable than human testimony, nor given evidentiary presumptions.30 “One presumption that may apply to computers is the presumption that a machine is presumed to be in working order. In the context of digital evidence, however, it is pertinent to be aware of the imperfections inherent in the way computers function, and how digital evidence is prone to alteration. Evidence derived from a computer

---

25 _Peter Drucker, The New Realities_ 262 (1989) (“And biological process is not analytical. In a mechanical phenomenon the whole is equal to the sum of its parts and therefore capable of being understood by analysis. Biological phenomena are however ‘wholes.’ They are different from the sum of their parts.”).

26 _Warren Weaver, The Mathematics of Communication_, 181 Sci. Am. 11, 13 (1949) (“Information is . . . a measure of one’s freedom of choice in selecting a message. The greater this freedom of choice, and hence the greater the information, the greater is the uncertainty that the message actually is some particular one. Thus greater freedom of choice, greater uncertainty, greater information go hand in hand.”). _See generally Vining, supra_ note 21, at 281 (“Against the constant fading of the conditions of authority is what comes from law that pushes toward the personal and a context of decision making in which the personal can be recognized, recognition of the personal being the only entry to the experience of authority.”).

27 For a discussion about how the examples of electronic signatures and networked communications are challenged by a lack of evidence in proving who clicked the button or caused the particular signature to be made, _see Stephen Mason, Electronic Signatures in Law_, 189 (Institute of Advanced Legal Studies, 4th edn, 2016). _See also_ Vining, _supra_ note 21, at 281 (1995) (“And the central concern of law, atheoretical, pretheoretical, is then connection of value and responsible mind, for value not connected by mind to responsible belief is mirage, nothing, vanishing when questioned or sought.”).


30 Mason, _supra_ note 27, at 386. For a detailed discussion on the presumption that computers are reliable and judicial notice in respect of software, and why such a presumption is not appropriate, see _Stephen Mason and Daniel Seng, editors, Electronic Evidence_ (Institute of Advanced Legal Studies, 4th edn, 2017), chapter 6.
must be admissible, authentic, accurate and complete in the same way as any other form of evidence.”

22. Within the context of litigation, a bank, for example, will make every effort to refrain from revealing evidence of its software systems and the rationale for its reasoning. In so doing, the bank will usually ask an adjudicator to accept their assurances without providing evidence to sustain their claims, and judges will accept such assurances in the absence of any evidence. This illustrates the comment by Harbison, that “Trust, by definition, is not a guarantee. Therefore an approach to understanding trust is also one of assessing risk.”

23. Digital technologies must be deployed in such a manner as to link persons to actions and thereby provide a necessary immutable reference for proving the authenticity of digital information over time.

24. The communication of one item of software with another item of software governs much of what we do when interacting with machines controlled by software.

25. Software code is subject to human technical mistakes and misperceptions of business and legal requirements. The open distributed system of communications with which we interact is very complex and subject to human design error. It is important for those involved with the law to recognize that human beings write the software that controls machines – software is the witness. People make mistakes, and errors occur when writing software.

---

31 Mason, supra note 27, at 385-86.
32 For an example of the assurances accepted by a judge without any evidence, see the Norwegian case of Bernt Petter Jørgensen v DnB NOR Bank ASA, Trondheim District Court, 24 September 2004, 9 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REV 117 – 123 (2012); Maryke Silalahi Nuth, Unauthorized use of bank cards with or without the PIN: a lost case for the customer?, 9 DIGITAL EVIDENCE AND ELECTRONIC SIGNATURE LAW REVIEW 95 – 101 (2012).
34 Mason, supra note 27. As an example, electronic signatures and networked communications are challenged by a lack of direct evidence.
35 Of relevance is the following observation in GEORGE DYSON, DARWIN AMONG THE MACHINES 10 – 13 (1997). (“Although our attention has been focused on the growth of computer networks as a medium for communication among human beings, beneath the surface lies a far more extensive growth in communication among machines. Everything that human beings are doing to make it easier to operate computer networks is at the same time, but for different reasons, making it easier for computer networks to operate human beings.”)
36 The untrustworthiness of evidence generated by software code and the platforms upon which it runs is examined by Sergey Bratus, Ashlyn Lembree, and Anna Shubina, in Software on the Witness Stand: What Should It Take for Us to Trust It?, Alessandro Acquisti, Sean W. Smith and Ahmad-Reza Sadeghi, eds, TRUST AND TRUSTWORTHY COMPUTING, LECTURE NOTES IN COMPUTER SCIENCE VOLUME 6101, 396 – 416 (Springer Berlin Heidelberg, 2010), available at http://www.cs.dartmouth.edu/~sergey/trusting-e-evidence.pdf; see also Mason and Seng, supra note 30, chapter 5 ‘Software code as the witness’.
37 For a discussion of the imperfections of software in the context of the legal presumption that a machine controlled by software is reliable, see Mason and Seng, supra note 30, chapter 6; see also the general discussions in GEORGE L. PAUL, FOUNDATIONS OF DIGITAL EVIDENCE 131-50 (2008):
26. Despite that fact that software code is subject to human technical mistakes, legal systems give presumptions of liability that renders difficult legal challenge and analysis of causation.\(^\text{38}\)

C. Article 29

(1) Everyone has duties to the community in which alone the free and full development of his personality is possible. (2) In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society. (3) These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations.

27. Choices made by software coders that control our rights and ability to act in cyberspace reflect the goals and values of the coders and not necessarily the users. Most users do not have any knowledge of software or its biases and value choices embedded by those who write code or of how much software controls our lives.\(^\text{39}\) When machines controlled by software fail, it is often the case that the user is blamed for the failure, rather than the relying party or service provider, which in turn has developed its own software or purchased software or software systems that are considered to be suitable for using personal information.\(^\text{40}\)

---

\(^{38}\) For a discussion of the undue presumption of reliability of computers and software code, see Mason supra note 28, at 222-4.

\(^{39}\) For a discussion of software coders’ hidden biases and value choices with respect to privacy and risk embedded in software, see Lawrence Lessig, Code is Law, Harvard Magazine, January-February 2000, available at http://harvardmagazine.com/2000/01/code-is-law-html. "The code regulates. It implements values, or not. It enables freedoms, or disables them. It protects privacy, or promotes monitoring. People choose how the code does these things. People write the code. Thus the choice is not whether people will decide how cyberspace regulates. People – coders – will. The only choice is whether we collectively will have a role in their choice – and thus in determining how these values regulate – or whether collectively we will allow the coders to select our values for us."

\(^{40}\) Vining, supra note 14, at 25 (1986).
28. All human organization requires authority. But by removing community as well as the human person as an actor with free will and choice, machines and systems controlled by software code become authoritarian and impersonal.41

29. The order in all systems presupposes that their components stand in specific communicative relations to one another.42 Therefore, in ordering both human to machine and machine to machine communications, we need shared community with a common system for configuring human rights in software code.43

30. We argue that if a party is encouraged to rely on software code in the machine-mediated information economy, it is imperative that a trust framework or code of conduct, such as the various United Nations model laws in the e-commerce context, provides adequately for individual autonomy, the establishment of reciprocal and enforceable rights and duties, and objectively and fairly addresses privacy risk.

31. The law must hold, and be seen to hold, the various participants in the cyber chain accountable for the systems they put in place. An effective remedy must be made available to take into account the nature of the loss. This does not necessarily mean that the usual method of assessing loss is suitable for the loss of personal information. The data protection laws in place in the European Union, for instance, generally do not provide any effective remedies to ordinary people. An organization might be subject to an administrative fine for failing to secure personal data, but the individual has little option other than to hope that their information will not be used to their disadvantage.44

41 Authentic relations arise between persons and require a shared interactive community and common language. See HAROLD BERMAN (EDITED BY JOHN WITTE, JR.), LAW AND LANGUAGE: EFFECTIVE SYMBOLS OF COMMUNITY (2013) (language is a process of creating community and social relations as well as being a process of exchange, interaction, and transferring meaning.) See also Drucker supra note 21, at 260 (“For communication to be effective there has to be both information and meaning. And meaning requires communion...Communion, however, does not work well if the group is very large. It requires constant reaffirmation. It requires the ability to interpret. It requires a community.”).

42 See PIERRE DE LATIL, THINKING BY MACHINE: A STUDY OF CYBERNETICS 206 – 207 (1957): “The amount of information that can be transmitted depends on a measure of the degree of order ... Any signal necessarily involves differentiation. A high degree of differentiation allows all sorts of codified variations and hence a large amount of information can be carried.”

43 Dyson, supra note 35, at 158 – 168. See also Drucker, supra note 21, at 264 (“Indeed, the new realities with which this book deals are configurations and as such call for perception as much as for analysis...But contemporary philosophers no longer focus on Kant’s concerns. They deal with configurations – with signs and symbols, with patterns, with myth, with language. They deal with perception. Thus the shift from the mechanical to the biological universe will eventually require a new philosophical synthesis.”).

44 See Mason, supra note 29, at 83 (“Failing to provide for effective and a robust means by which individuals can protect their privacy and obtain effective remedies –and the ineffectiveness of various data protection legislation across the world demonstrates the inability of governments to provide for the protection of data—means that powerful commercial interests will, in effect, become an even more significant source of influence in the future, because of the massive range of personal information they have at their disposal, regardless of how it is obtained.”).
32. Anonymity is the central characteristic of the machine-mediated information age. In this respect, an important issue is the degree of ‘trust’ that we can expect when interacting with a machine that is controlled by software.45

33. Associated with the machine-mediated information age has been a loss of both shared community and the capacity to make community.46

III. Human Rights and Digital Technologies: Emerging Recognition and Enforcement Mechanisms

34. In response, both the private and public sectors are now using Lex Informatica approaches to guide system designs and network architecture with a human rights-oriented paradigm.47 Emerging programs and policies are designed to foster the configuration of software code to enable human agency, human autonomy, and subjective or claim rights.48

A. Configuring Human Agency

35. To provide for the ability of an individual to control access to and the use of personal data for authentication purposes, we argue that users need autonomy of action as rights holders. The user-centric identity model is emerging as a Lex Informatica identity policy method to achieve this.49

36. The possibility of leveraging the blockchain to enhance informational privacy is being explored. Several organizations are promoting the concept of self-sovereign identities.50 With this concept, the

45 Ed Gerck, Toward Real-World Models of Trust: Reliance on Received Information (1997), available at http://mcwg.org/mcg-mirror/trustdef.htm. (“Trust in cyberspace (e.g., between machines) is defined and is based on the same notion of trust, as a form of reliance, that we have been using for millennia between humans and in business.”)

46 Berman, supra note 41, at 48.

47 Reidenberg, supra note 3, at 586.

48 For an optimistic assessment, see Nicholas Negroponte, Being Digital 228-9 (1995) (“Bits are not edible, in that sense they cannot stop hunger. Computers are not moral; they cannot resolve complex issues like the rights to life and to death. But being digital, nevertheless, does give much cause for optimism. Like a force of nature, the digital age cannot be denied or stopped. It has four very powerful qualities that will result in its ultimate triumph: decentralizing, globalizing, harmonizing, and empowering.”).

49 For a representative description of user-centric identity, see the white paper Issues for Responsible User-Centric Identity 2 (Center for Democracy & Technology, November 2009, Version 1.0), available at https://cdt.org/insight/cdt-discusses-key-policies-issues-surrounding-user-centric-identity-management/ (“This term refers to systems where users, rather than service providers, control their identity credentials.”).
decentralized and distributed trust afforded by blockchain ledgers enables the creation of user-created and controlled digital identities.\textsuperscript{51}

37. The United Nations High Commissioner for Refugees (UNHCR), in collaboration with the World Bank, has launched an effort to provide legal identities to all individuals who are stateless or lacking a birth registration.\textsuperscript{52} To further enhance user control over digital identities and the sharing of personal information for these persons to obtain social services, the UNHCR is looking to leverage the European Union funded LIGHTest Project to enable an authoritative trust infrastructure.\textsuperscript{53}

\textbf{B. Configuring Human Autonomy}

38. The User-Managed Access (UMA) access sharing protocol,\textsuperscript{54} based on permission tokens that can be used as devices to license access rights with respect to personal digital assets collected and stored by devices, apps, and databases, provides an authoritative basis for communicating access consent as economic value. After integrating the UMA access sharing protocol, community trust can be built on legitimate and internationally recognized licenses that signal both to sending and relying parties a common understanding of legal relationships with respect to personal data. UMA permission tokens can be used as abstract contracts or credit devices for licensing informational rights in personally identifiable information, including informed consent to health information.\textsuperscript{55}

39. Legal consent issues are especially at issue with cross-border data transfers requirements such as the GDPR\textsuperscript{56} and the associated sharing of personal data for identity authentication purposes.\textsuperscript{57} A

\begin{itemize}
  \item \textsuperscript{50} Adam Piore, \textit{Can Blockchain Finally give us the Digital Privacy we Deserve?} Newsweek, February 22, 2019, (describing the current rate of identity theft as an “identity crisis”) available at https://www.newsweek.com/2019/03/08/can-blockchain-finally-give-us-digital-privacy-we-deserve-1340689.html.
  \item \textsuperscript{53} A description of LIGHTest Project is available at https://www.lightest.eu/ and https://www.lightest-community.org/.
  \item \textsuperscript{54} The UMA Version 2.0 protocol specifications can be viewed at: https://kantarainitiative.org/reports-recommendations/.
  \item \textsuperscript{55} UMA has been developed under the auspices of the Kantara Initiative.
  \item \textsuperscript{56} For a discussion of the licensing of informational rights by individuals, see Mark A. Hall, \textit{Property, Privacy, and the Pursuit of Interconnected Electronic Medical Records}, 95 IOWA L. REV. 631, 660 (2010) ("People should be able themselves, or through their agents, to authorize access to and use of their medical information for financial rewards, and these licenses should be transferable."). \textit{See also}, Pamela Samuelson, \textit{Privacy as Intellectual Property}, 52 STAN. L. REV. 1125, 1134 (2000) (endorsing a licensing approach to the protection of information rights in personal data).
  \item \textsuperscript{58} See Article 1(f)(ii) of the eIDAS Regulation, available at http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2014.257.01.0073.01.ENG.
\end{itemize}
consent receipt is a record of a consent provided to an individual at the point in a person agrees to the sharing of personal information. Its purpose is to capture the privacy policy associated with the personal information so that the consent receipt can be easily used to communicate and manage consent and sharing of personal information once it is provided.⁵⁸

C. Configuring Human Authority

40. Legal frameworks are now being developed that define and clarify the liability of all digital identity service providers. As an example, the Virginia digital identity law reflects public support for the creation of a market of identity service providers based on clear bases for liability.⁵⁹ By supporting a user-centric identity architecture for access to online services, the law is intended to provide Virginia citizens with a means of controlling their digital identities. The law also provides a basis for a private right of action against identity service providers for unauthorized use and transfer of personal information.

41. Related to the Virginia Identity Law as well as the eIDAS⁶⁰ in the European Union, The United Nations Commission on International Trade Law, Working Group IV, is currently preparing a draft model law for cross-border recognition of identity credentials and related trust services.⁶¹

42. Building on the credit union model, data cooperatives with fiduciary obligations to members provide an additional means for individuals to exercise a control over personal data.⁶² A data cooperative can manage, curate and protect access to the personal data of citizen members. Furthermore, the data cooperative can run internal analytical programs in order to obtain insights regarding the well-being of its members. Armed with these insights, the data cooperative is authorized to negotiate services and discounts for its members.

⁵⁸ For a discussion of consent receipts, see the Kantara Initiative program, available at https://kantarainitiative.org/confluence/display/infosharing/Consent+Receipt+Specification.
⁶⁰ The eIDAS of the European Union can be viewed at https://ec.europa.eu/futurium/en/content/eidas-regulation-regulation-eu-ndeg9102014.
⁶² The concept of data cooperatives has been developed at the Massachusetts Institute of Technology Media Lab. For a detailed discussion, see Thomas Hardjono and Sandy Pentland, Data Cooperatives: Towards a Foundation for Decentralized Personal Data Management, (Cornell University, May 21, 2019) available at https://arxiv.org/abs/1905.08819.
43. Legal recognition for the use of video witnessing as the equivalent of personal appearance has emerged with online notarization in the United States. The Law Commission of the United Kingdom has recently recommended that formal consideration be given for giving legal recognition to video witnessing as a method of satisfying a requirement for a personal appearance of a document signer.

IV. Conclusion

44. This paper addresses several important legal and policy issues facing the overall challenge of recognizing and enforcing human rights in the machine-mediated age governed by software code. We contend that digital technologies must be configured by the UDHR paradigm to enable human agency, autonomy, and claim rights. Further, we contend that it is necessary in the digital age to provide for an effective and robust means by which individuals can obtain effective remedies.

45. Human agency, autonomy, and authority are three experiential realizations of digital technologies when configured in a human rights paradigm. From the legal perspective, the human rights paradigm is intended to forge information processes that are authoritative and prevent the authoritarian.

Timothy Reiniger is an attorney specializing in information law and policy (licensed to practice in California, the District of Columbia, Maine, and New Hampshire). He has served as an ABA-appointed advisor to the Uniform Law Commission and is an author of both the Virginia online notarization law (2011) and the Virginia digital identity law (2015). As a former Executive Director of the National Notary Association, he is recognized as an expert in notarial law, providing testimony on this subject.

63 Beginning with Virginia in 2011, twenty-two state jurisdictions in the United States have now enacted laws authorizing a remote appearance before a notary by means of audio-video communication technologies. For a detailed discussion, see Timothy Reiniger, Developments in Information Governance, the Emergence of Online Notarization, ABA INFORMATION LAW JOURNAL Vol. 9 Issue 4, 10-18 (Autumn 2018), available at https://www.asnnotary.org/files/Online%20Notarization%20%20INFORMATION_LAW_JOURNAL-volume9_issue4%202018.pdf. For a discussion of online notarization and video witnessing in the probate context, see Michael Chodos (General Counsel of Notarize) and Timothy Reiniger, The Emergence of the Online Notary: Implications for the Probate Bar, PROBATE & PROPERTY (A PUBLICATION OF THE REAL PROPERTY, TRUST AND ESTATE LAW SECTION, ABA), Vol. 33, No. 4, 59-62 (July/August 2019).


65 The authors praise the United Nations for seeking to extend human rights principles to the digital technologies. The UDHR, like the lighthouse that provides safety to vessels, serves as a beacon providing safety to human beings in the machine-mediated age government by software code. Accordingly, we find the following passage as an apt close to this submission:

"Sail on!" it says, "sail on, ye stately ships!
And with your floating bridge the ocean span;
Be mine to guard this light from all eclipse,
Be yours to bring man nearer unto man!"
-- Henry Wadsworth Longfellow (The Lighthouse, 1849)
before the United States Congress and over twenty state legislatures. Currently, he serves on the advisory board of the EU’s LIGHTest Project (Horizon 2020) and is Director of the Reiniger LLC in Cape Elizabeth, Maine. He can be reached at tim@reinigerllc.com.

Stephen Mason is barrister. He was invited by the Law Commission to be a member of the Advisory Panel of experts for the report entitled Electronic execution of documents. Stephen the author of the open source practitioner text Electronic Signatures in Law (4th edn, 2016), and the co-editor, with Daniel Seng, of the open source practitioner text Electronic Evidence (4th edn, 2017), and the editor of International Electronic Evidence (2008). He is the founder of the international open source journal Digital Evidence and Electronic Signature Law Review. He can be reached at stephenmason@stephenmason.co.uk.
Ephemeral Messaging Presents New E-Discovery Challenges

By Alexander B. Hastings, Michael Fletcher, and Edward H. Rippey

Information management and e-discovery seem to present a never-ending supply of challenges as technology develops, and the need to respond to these developments is ever present as vanishing messaging applications are exploding in popularity. Not only are these technologies used to convey personal messages, they are increasingly being used by companies and their employees to conduct business. Because these applications are “ephemeral” or create no lasting record of the communication, investigators and parties seeking information about a company’s practices may raise issues with the use of ephemeral platforms. The applications also implicate concerns regarding the proper retention of records that can lead to spoliation claims. Nonetheless, there are legitimate reasons that companies allow or even favor the use of ephemeral messaging platforms given the need to protect trade secrets and personal information from cybersecurity threats and in light of the growing proliferation of data that companies must manage. This article discusses the rise of these ephemeral messaging applications and the implications they may have for companies, including the potential need to address recent guidance from the Department of Justice (“DOJ”) regarding the use of these applications.

1. The Rise and Benefits of Ephemeral Messaging Applications

The impact that new messaging technologies will have on litigation and e-discovery has yet to be fully realized, but since Federal Rule of Civil Procedure 37(e) was amended in 2015, messaging technologies have taken another leap forward from the more simple instant messaging platforms of the past. In addition to the popular Snapchat application, which is used primarily by teenagers and young adults, there are now many applications in this space, including Wickr, WhatsApp, WeChat, Telegram, Cover Me, and Confide. Some new ephemeral messaging platforms, like Confide, specifically target companies and professionals. The developers of Confide advertise that the application “uses military-grade end-to-end encryption to keep your messages safe and ensure that they can only be read by the intended recipients.” The technology also makes messages “disappear forever after they are read once.”

Although ephemeral messaging is often associated with conveying illicit or scandalous messages, there are legitimate professional and corporate uses of ephemeral messaging. For instance, companies today generate a vast amount of data, and storing this data can be costly and create additional litigation risks. Allowing employees to use ephemeral messaging applications can help companies reduce the amount of duplicative data that is stored, thereby reducing the cost of overall data storage.
In addition, as long as the company is complying with applicable record retention requirements, disposing of unnecessary documents and communications provides another route for a company to minimize the cost of e-discovery. Ephemeral messaging applications also can provide another level of security from hackers that persistently target corporations’ data. If sensitive business data is kept in fewer places, there is a lower probability of cybercriminals successfully accessing it. Finally, when communicating with employees abroad, encrypted and ephemeral messaging applications can provide some protection for sensitive communications (e.g., communications that involve trade secrets or proprietary information).

2. Government Treatment of Ephemeral Messaging Apps in White Collar Investigations

Given the legitimate corporate uses of ephemeral messaging applications in some contexts, it is reasonable that a company may, in certain contexts, want or allow its employees to use ephemeral messaging applications. Nonetheless, it is both helpful and important for companies to understand how investigators may view the use of ephemeral messaging applications as the use of these applications could have a significant impact on the government’s view of the investigation and remediation measures.

For instance, with respect to Foreign Corrupt Practices Act (“FCPA”) investigations, the DOJ can award companies full or partial cooperation credit for voluntary self-disclosing compliance issues and timely and appropriately remediating those issues, which can ultimately reduce the penalty levied against the company. The guidelines for cooperation, articulated in the FCPA Corporate Enforcement Policy, address ephemeral messaging applications. Until recently, this policy stated that receiving full remediation credit required companies to “prohibit[] the improper destruction or deletion of business records, including prohibiting employees from using software that generates but does not appropriately retain business records or communications.” This portion of the policy resulted in significant concern for companies in light of the difficulties of retaining communications made through ephemeral messaging applications.

In March 2019, the DOJ updated the policy and appeared to dial back its apparent complete prohibition of ephemeral messaging applications. The policy now states that in order to receive full credit for timely and appropriate remediation, companies are required to implement “appropriate guidance and controls” on employees’ use of personal communications and ephemeral messaging

---

1 FCPA Corporate Enforcement Policy, Department of Justice, available online at https://www.justice.gov/criminal-fraud/file/838416/download. The FCPA enforcement policy applies to all white collar matters handled by the DOJ Criminal Division. See Jonathan S. Kolodner, Lisa Vicens, and Lorena Michelen, DOJ Updates FCPA Corporate Enforcement Policy, Program on Corporate Compliance and Enforcement at New York University School of Law, available online at https://wp.nyu.edu/compliance_enforcement/2019/04/10/doj-updates-fcpa-corporate-enforcement-policy/.

systems. This “appropriate guidance and controls” standard with respect to a company’s use of ephemeral messaging seems to codify a “risk based approach” that the DOJ signaled that it would like companies to take with respect to messaging applications. Given how recently the guidance changed, the meaning of “appropriate guidance and controls” has yet to be clarified through subsequent DOJ statements or through the DOJ’s enforcement actions. Therefore, until the DOJ provides further guidance on what it will accept as adequate guidance and controls on ephemeral messaging applications, companies would be well advised to document employee guidance regarding these applications and be prepared to explain to the DOJ the controls they have implemented with respect to messaging platforms.

3. Implications for Companies

Companies—particularly those subject to the DOJ’s new policy or under a legal hold—should account for employees’ actual or potential use of ephemeral messaging applications, ideally by addressing them in the company’s information management policy. Indeed, even though such applications may be used for legitimate business purposes, a layperson (such as a juror) may draw certain assumptions from a company’s use of ephemeral messaging applications. For instance, courts have allowed parties to present evidence and argument at trial that a company’s use of ephemeral communications was the reason that the opposing party was not able to collect more information during discovery. Unless a company is able to present a consistent and clear approach for employees’ legitimate use of ephemeral messaging applications, these arguments may leave jurors (and the public) with a misimpression of the legitimacy of a company’s use of these messaging platforms. Therefore, it can be important to account for these applications within a company’s information management policies.

When addressing ephemeral messaging applications, companies should assess what guidelines are realistic. For instance, an outright prohibition on these applications may not be feasible and could lead to a culture of non-compliance with an information management policy should employees find that they have to circumvent a ban on these applications in order to effectively perform their job functions. As a result, companies would typically be well advised to lay out clearly for employees the expectations regarding these applications and the types of communications that are permitted and prohibited. For instance, a company may choose to generally allow the use of these applications for non-substantive discussions, such as meeting arrangements or lunch plans, while discouraging or prohibiting their use for substantive business discussions. In addition, because some ephemeral messaging applications now allow a user to disable the “ephemeral” nature of the messages and retain them for longer periods, companies may encourage or require employees to use such features on a perpetual basis or at least when an employee is subject to a legal hold.

4 DOJ Revises FCPA Corporate Enforcement Policy, supra at 55.
5 Id.
When implementing guidance regarding ephemeral messaging applications, companies should also consider personal devices. Many employees use ephemeral messaging applications for personal reasons and may push back on company policies that restrict the personal use of such applications on devices connected to a company’s network. Additionally, in the case of multinational corporations, companies should be aware that different messaging platforms are more prevalently used in certain regions. Therefore, it may be wise for a company to assess the landscape and then to realistically set standards for what behavior is acceptable.

In short, ephemeral messaging applications appear to be growing in popularity and technical capability. Similar to the instant messaging platforms that the e-discovery community responded to several years ago, the approach to ephemeral messaging applications is likely to remain a fluid area with companies adopting a host of different responses. That said, whether a company is seeking compliance with the new DOJ policy or simply attempting to account for this new technology in its information management systems, most companies would be well advised to establish a clear policy outlining the acceptable use of ephemeral messaging applications and be prepared to explain the policy to government agencies or opposing parties.

**Alexander Hastings** (ahastings@cov.com) is a Special Counsel at Covington & Burling LLP and member of the firm’s E-Discovery and Information Management Group.

**Michael Fletcher** was an associate at the firm.

**Edward Rippey** (erippey@cov.com) is a partner at the firm, handles complex commercial litigation, and is Chair of the E-Discovery and Information Management Practice Group.