THE AUTOMATION PARADOX IN LITIGATION: THE INADEQUACY OF PROCEDURE AND EVIDENCE LAW TO MANAGE ELECTRONIC EVIDENCE GENERATED BY THE 'INTERNET OF THINGS' IN CIVIL DISPUTES

DAVID CARUSO,* MICHAEL LEGG,** JORDAN PHOUSTANIS***

Recent advances in technology and a collective appetite for technological integration have resulted in the design of many 'everyday' objects, devices, machines, and buildings that incorporate data gathering, handling and transmission technology, commonly referred to as the Internet of Things. This article examines the procedural and evidential implications and challenges of collecting and exchanging electronically stored information gathered by these everyday objects. In particular, the article examines the discovery of that data in the context of court proceedings, and highlights the novel challenges presented by the format and location of the data. The article also considers the way in which this data is presented in court and issues relating to the admissibility and proper weight of evidence extracted from the Internet of Things. In particular, the article focuses on the circumstances in which the hearsay rule may affect the furnishing of such data, and how issues of identity and provenance are affected by the unique format and character of the evidence.

I INTRODUCTION

Advances in technology and a collective appetite for technological integration have resulted in the design of many 'every-day' objects, devices, machines and buildings that incorporate data gathering, handling and transmission technology. These things have not previously been computerised or connected to an information exchange network. The technology, capable of continuously perceiving, monitoring, recording and transmitting information, represents a substantial advancement in both the function and pervasiveness of technology in daily private and professional life. Technology that automatically gathers and records data from the external environment has and will continue to increase the volume of multiplatform information that would previously have been unobserved, unmeasured and unrecorded. The advent of autonomous technology which is interlinked to human need by network has been referred to as 'ubiquitous computing' and 'ambient intelligence'.[1] It has also been recognised as the 'third wave' of computing. A consequence of the advent of the third wave of computing is that the volume of information that is recorded and stored is increasing. Furthermore, the proportion of available information that is recorded and stored as data is also increasing, resulting

* Director, Litigation Law Unit, University of Adelaide; Senior Lecturer, Adelaide Law School.
** Professor, UNSW Law and Director of the Law Society of New South Wales Future of Law and Innovation in the Profession (FLIP) research stream at UNSW Law.
*** Solicitor, Herbert Smith Freehills.

1 See Kayleen Manwaring and Roger Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (2015) 31(5) *Computer Law and Security Review* 586; Kayleen Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2017) 22 *Deakin Law Review* 53.

in the availability of more contemporaneous evidence to issues in question. It has been estimated that data generated by these objects, devices, machines and buildings – often collectively referred to as the 'Internet of Things' ('IoT') – will account for about 10 percent of the data on Earth by 2020.[2]

Our focus is the consequence of third wave computing for litigation. In Part II, we explain the third wave of computing and the manner in which the IoT operates. Part III examines the retrieval, handling and discovery of that data in the context of court proceedings, and highlights the novel challenges presented by the format and location of the data. We then consider the presentation of IoT-derived electronic evidence in court and issues relating to its admissibility. In Part IV, we consider the circumstances in which the hearsay rule may affect the furnishing of such data, and Part V examines how issues of identity and provenance are affected by the unique format and character of the evidence. We conclude that IoT-derived evidence presents significant challenges to present legal tests and methods for its authentication.

II THE INTERNET OF THINGS

A *Third Wave eObjects*

The 'third wave' of computing involves the insertion of intuitive devices into our everyday devices and surrounds. This technology is intuitive in that it independently responds to and monitors our daily needs. The broader effect of this third wave is the embedding of data gathering, handling and transmission devices in a variety of objects, devices, machines, buildings and environments that previously were neither computerised nor connected to the internet or local information exchange network.[3] An epitomical example is a Fitbit, a fitness tracking watch, which monitors and records the wearer's heart rate and geolocation and transmits this information via Bluetooth technology to another mobile device, and to the internet, via remote server. This is obviously not the traditional analogue function of the watch.

Third wave devices have sensory technology with the capacity to transmit, via network, data gathered by the device to other devices or storage platforms. These devices are commonly referred to as enhanced objects ('eObjects'). An eObject has been defined as an 'object that is not inherently computerised, but into which has been embedded one or more computer processors with data-collection, data-handling and data-communication capabilities'.[4]

The IoT provides a collective term for eObjects. The IoT may be understood as a network connecting eObjects. The network, usually the internet, facilitates the transmission of data gathered by eObjects to other devices, which are often also

---

2 Anthony Adshead, 'Data set to grow 10-fold by 2020 as internet of things takes off', *ComputerWeekly.com* (online, 9 April 2014) <https://www.computerweekly.com/news/2240217788/data-set-to-grow-10-fold-by-2020-as-internet-of-things-takes-off>.

3 Texas Instruments Inc has classified eObjects and applications into six categories: wearables, health care, building and home automation, smart manufacturing, smart cities and automotive: Texas Instruments, 'Internet of Things', (Web Page) <http://www.ti.com/ww/en/internet_of_things/iot-applications.html>.

4 Kayleen Manwaring and Roger Clarke, 'Surfing the Third Wave of Computing: A Framework for Research Into eObjects' (2015) 31(5) *Computer Law and Security Review* 586, 599.

eObjects or data storage devices such as servers, mobile telephones, and hard drives. Those devices retain their 'traditional' or 'primary' functionality and are embedded with electronics, software, sensors, and network connectivity that enables them to collect, record and communicate data (which may concern or relate to the function or performance of the device).[5] To illustrate, many of the appliances within a typical residential apartment may be eObjects, including the air-conditioner, lights, refrigerator, and robotic vacuum cleaner. The electronically stored information ('ESI'), generated by eObjects, which are connected by the IoT, is a database regarding, for example, the lifestyle conditions and habits of the occupants of the residence.

The IoT progresses network computing beyond two-way person-to-person interactions to exchanges between persons and machines, and machine-to-machine interactions.[6] The IoT has significance for the commercial applications that it can facilitate. It also provides 'unprecedented visibility into people, the physical world they occupy and the interaction between the two'.[7]

This database – the ESI – is the information trove for discovery and the trial. Enhanced objects are the means to that value. In the following discussion, we examine the ESI generated from eObjects in the context of information gathering as part of the pre-trial process, namely through the use of court discovery and subpoena processes in the Federal Court of Australia[8] and, with respect to its admissibility, under the Australian Uniform Evidence Law ('UEL').[9]

B *ESI generated by the IoT*

ESI is an elastic term in the digital age where new and varied devices are increasingly capacitated to produce and store electronic data. ESI may be divided into three categories. First, data resulting from active human input to an electronic device, for example, emails, text messages and like messages, digital scale or speed camera read outs. Second, data resulting from passive human input to an electronic device, for example, data on geographic location collected by carrying a mobile phone, or heartrate and personal vitals collected by a wrist-worn fitness monitor. Third, data resulting from operation of pre-programmed automated devices, which operate independently of human input, for example, temperature data gathered by a computerised air conditioner or refrigerator. An eObject pre-programmed to gather data in the manner of the third category may, however, be overridden by active human input. For example, persons may change or interrupt programmed settings.

The first category of ESI, which is generated by active human input and operation of devices, is familiar to courts (and society generally) as a category of data produced from the use of technology. The human plays an active and direct role in producing and transmitting the data. The technology provides a conversion and delivery method

---

5 International Telecommunications Union, *Overview of the Internet of Things – Recommendation ITU-T Y.2060* (06/2012); Telstra Corporation Limited, *Millennials, Mobiles and Money* (2016) 56.

6 Andrew Whitmore, Anurag Agarway and Li Da Xu, 'The Internet of Things – A Survey of Topics and Trends' (2015) 17(2) *Information Systems Frontiers* 261, 261.

7 Telstra Corporation Limited, *Millennials, Mobiles and Money* (2016) 56.

8 *Federal Court of Australia Act 1976* (Cth); *Federal Court Rules 2011* (Cth) ('*FCR*').

9 *Evidence Act 1995* (Cth); *Evidence Act 1995* (NSW); *Evidence Act 2008* (Vic); *Evidence Act 2001* (Tas). All sections of law referenced herein are to the UEL, unless otherwise stated.

for the human input, as in the case of sending an email, or the technology may perform more readily discernible,[10] calculated functions as a result of human command, as in the case of digital scales or speed cameras. In either example, the ESI that may be later sourced is data that was produced by direct and deliberate human operation of the device.

The second and third categories of ESI have the shared characteristic of being recorded without direct or active human input to generate the particular data. ESI gathered by the passive operation of technology is the purview of eObjects. Assuming a power source, the eObject is programmed to capture data of particular types without the need for ongoing or direct human input. The passive involvement of the human element in eObjects dramatically expands the circumstances and environments through which eObjects can capture data. This accounts for their (i) mobility, (ii) volatility and vulnerability, and (iii) autonomy in ways unique from first and second wave computing.[11] These aspects are elaborated on below.

1 *Mobility*

Mobility is a characteristic of many eObjects. The commercial attraction of the eObject system often relates to its mobility for the consumer. Mobility is assisted by the expansion of wireless networks which allow the eObject to remain connected, for example, in outdoor settings or even in flight, which the need for hard-line internet connections previously excluded from network access. The miniaturisation of eObjects, especially as compared to the computing devices of the first wave, also enables their portability. The result is a pervasive network and portable eObjects that can remain operational and connected without interruption. Indeed, the primary reason for the interruption of many eObjects is the need for them to be recharged, and even this need is diminishing with the development of inexpensive portable charging devices. The data amassable from the uninterrupted recording and connectivity of eObjects, regardless of the environment, can increasingly provide a complete data set with respect to the matters the eObject is designed to capture, as well as, perhaps, matters that it was not designed to observe or capture. As technology improves, so too will the quality of the data captured, but the importance at present is the capacity of the eObject to capture a comprehensive and uninterrupted data set, owing to the mobility of the device.

2 *Volatility and vulnerability*

The observations made in respect of mobility require stable operational environments both for the eObject and the network to which it is connected. Ordinary experience dictates that networks, regardless of size (eg, home or office) or environment of operation (eg, indoor or outdoor), may function haphazardly and, accordingly, so too might the technology of the eObject itself. This will lessen as technology advances but, still, the operation of eObjects is potentially volatile. This volatility is more probable as a result of mobility. Mobility more readily permits changes in the circumstances and

---

10 Encoding obviously performs programmed, calculated functions to deliver even the most basic human to computer commands, such as converting type touches to electronic text, but because the keyboard letter touched appears directly on the visual platform, the computerised calculations are less discernible than technology which calculates unknown commands.

11 Kayleen Manwaring, 'Kickstarting Reconnection: An Approach to Legal Problems Arising from Emerging Technologies' (2017) 22 *Deakin Law Review* 53, 53.

environment of the human user, the eObject, and the IoT environment in which the eObject may be operating. The consequence is that their operation and captured data may be subject to flux and the changes that result may not be traceable or recorded. This can render the records of eObjects uncertain and raise evidential questions regarding the reliability of presented data to accurately demonstrate a state of affairs at a given time.[12]

The result of this volatility is that it may provide a basis for questioning the integrity of the data captured through an eObject. The eObject is, of course, also potentially vulnerable to direct and intentional interference or manipulation. Vulnerability and security concerns are heightened for eObjects, as they are typically less secure than analogue or immobile devices. They are more likely to be lost or stolen, or used by an unauthorised or unidentified operator in a physical sense (ie physical interference). They are also open to remote hacking and interference as a corollary of their network connectivity.[13] This direct potential for interference is the complement to the potential for indirect interference provided by mere mobility and raises the same questions, evidentially, for the integrity of the eObject-produced record.

3 *Autonomy*

Autonomy is the capability of eObjects to make decisions and initiate operation absent direct human operation or instruction to perform particular tasks. Autonomy is an increasingly prevalent characteristic of ambient technologies. The level of autonomy may be regarded as a continuum from, at the rudimentary level, the capacity to record and communicate data absent human instructions to do so, to, at the advanced level, the operation of the eObject itself based on programming, stimulus and/or independent data processing and decision-making.[14] The autonomous function of the eObject is governed, macroscopically, by source code. The source code is a set of instructions which the eObject effectively communicates to itself to take actions. The eObject tells various components of itself to take action based on the programming or sensory data captured by other parts of its constituent componentry and code. This gives rise to issues as to whether the ESI of eObjects ought to be subject to hearsay or analogous principles in the same way as human testimony, on account of the ESI being the testimony of the eObject, which may be based on other source code level communications of the eObject. There are questions as to whether further analogous principles need to be developed to manage these 'black box' dangers, but this is beyond the scope of this article.[15]

Technologically, eObjects are an advancement in the mobility of ambient networked devices capable of producing ESI. Enhanced objects, themselves, may be regarded as physical evidence. The eObject itself, however, is rarely the end but rather the start of an evidential interrogation. The coding of the eObject is pertinent to consideration of the ESI it records. For present purposes, we assume verified or verifiable source code.

---

12 Ibid 63.

13 Ibid 65.

14 Ibid 80.

15 For a comprehensive consideration see, Andrea Roth, 'Machine Testimony' (2017) 126(6) *Yale Law Review* 1972. For specified forensic applications, see also, Edward J Imwinkelried, 'Computer Source Code: A Source of the Growing Controversy Over the Reliability of Automated Forensic Techniques' (2017) 66 *DePaul Law Review* 97.

Our concerns are the procedural and evidential responses that should be taken to the uncertainty arising from the volatility and vulnerability inherent in the mobilised use of autonomous eObjects, which are discussed in detail below. We commence with the procedural issues.

III DISCLOSURE OF IOT-DERIVED ESI IN LITIGATION

The civil procedures of discovery and subpoenas are permitted in civil litigation because they increase the likelihood that a judgment or settlement will be correct and fair by facilitating knowledge of the facts. The ability to inspect an opponent's documents places parties on an equal footing and avoids 'trial by ambush'.[16] Despite the compelling arguments for discovery, it also necessitates cost and delay. In particular, approaches to discovery that leave 'no stone left unturned' can be oppressive and undermine the justice that discovery was meant to facilitate.[17]

The ESI generated from an eObject places the above competing views of discovery in stark relief, because the ESI provides increased visibility into the interaction between people and with the physical world they occupy.[18] This added visibility can provide data, and as discussed below, evidence, that can be crucial to accurate fact-finding and justice. However, the volume of ESI can also substantially increase the cost and burden of discovery.[19]

This section of the article examines the application of the procedures for discovery, and to a lesser extent subpoenas, to the ESI generated by eObjects that form part of the IoT. The third wave of computing generates substantial challenges for civil procedure, but those challenges are not as great as they might have been. This is because courts have previously had to grapple with the second wave of computing, or Web 2.0, when the internet went from providing static pages to providing two-way communication, most notably through social media.[20] The main focus of the analysis will be the rules and procedure of the Federal Court of Australia.

A *ESI and Documents*

The threshold question is whether ESI generated by eObjects is discoverable and, if so, what regimes or rules apply. Australian court rules dealing with discovery have typically focused on 'documents'. While historically the documents in issue were paper-based, the court rules have moved with the times and ESI will meet the definition of a document.[21] In the Federal Court of Australia, 'document' is defined in the Dictionary in Schedule 1 of the court rules as including:

---

16 Michael Legg, 'Discovery – A Comparative Approach to Reform' in Miiko Kumar and Michael Legg (eds), *Ten Years of the Civil Procedure Act 2005 (NSW)* (Thomson Reuters, 1st ed, 2015) 99.

17 *Expense Reduction Analysts Group Pty Ltd v Armstrong Strategic Management and Marketing Pty Ltd* (2013) 250 CLR 303, [47]; *Palavi v Radio 2UE Sydney Pty Ltd* [2011] NSWCA 264, [101].

18 Telstra Corporation Limited (n 5) 56.

19 *Australian Rugby Union Limited v Canterbury International (Australia) Pty Ltd (No 1)* [2012] FCA 497, [4]-[6].

20 Whitmore, Agarway and Xu (n 6) *261*.

21 Bernard Cairns, *Australian Civil Procedure* (Thomson Reuters, 11th ed, 2016) [10.170].

> (a) any record of information mentioned in the definition of document in Pt 1 of the Dictionary to the *Evidence Act 1995* (Cth); and (b) any other material, data or information stored or recorded by mechanical or electronic means.[22]

The Evidence Act definition is discussed below in relation to the UEL. However, data stored or recorded by electronic means would capture ESI created by an eObject.

B *ESI Relevant to Issues in the Proceedings*

While ESI is subject to discovery, the more specific question is when ESI from an eObject may be sufficiently relevant to an issue in proceedings that an order for discovery would be made.[23] Many courts have refined the general approach of requiring relevance by imposing stricter standards so that litigation is conducted in a manner that reduces cost and delay.[24] In the Federal Court, 'standard' discovery may be obtained for documents that are 'directly relevant to the issues raised by the pleadings or in the affidavits'.[25] This requirement is discussed further below. Similarly, ESI may be the subject of a subpoena provided the data being sought is both relevant to the proceedings and sufficiently described.[26]

So how might IoT data be used in litigation so that it might be subject to discovery, or a subpoena? Data from personal devices, cars and homes could be used to determine the location of a person. Most modern cars are equipped with a 'global positioning system' ('GPS'). Cell towers record the time that a mobile phone user passes by.[27] The thermostat in a house can record the presence of a person in specific rooms in their home, thus creating a record of occupancy.[28] The radio-frequency identification ('RFID') tags on inventory, assets and even employees' identification badges can be tracked to determine location.[29]

Vehicle data could also be used to determine if an accident was due to a mechanical fault, driver error or fatigue. Data from residential and commercial buildings may be used to detect whether windows and doors were locked or opened at a particular time so as to assist in insurance claims. Data from an internet-connected refrigerator might provide evidence about the condition of a comestible suspected of causing food

---

22 *Federal Court Rules 2011* (Cth) (*FCR)* sch 1 (definition of 'document').

23 Cairns (n 21) [10.100]-[10.130].

24 See Legg (n 16) 104-109 discussing the scope of discovery in Australia, the United Kingdom and the United States of America.

25 *FCR* r 20.14. Directly relevant is further defined as meaning that the document meets at least one of the following criteria: (a) the documents are those on which the party intends to rely; (b) the documents adversely affect the party's own case; (c) the documents support another party's case; (d) the documents adversely affect another party's case.

26 Miiko Kumar, Michael Legg and Ilija Vickovich, *Civil Procedure in New South Wales* (Thomson Reuters, 3rd ed, 2016) [12.390].

27 Samuel Greengard, *The Internet of Things* (MIT Press, 1st ed, 2015) 60-61.

28 Dennis Kennedy, 'Preparing for the "Internet of Things"*', ABA Journal*, 1 July 2014.

29 Greengard (n 27) 62. RFID uses electromagnetic fields to automatically identify and track tags attached to objects. Passive tags collect energy from a nearby RFID reader's interrogating radio waves. Active tags have a local power source (such as a battery) and may operate hundreds of meters from the RFID reader.

poisoning.[30] Similarly, in logistics, monitoring of shipping conditions could detect if items such as food become too hot or too cold at any point.[31]

The IoT could allow for a home monitoring system for elderly care which combines monitoring of medication and a patient's vital signs with an ability to communicate so as to order more medication when needed or, alert doctors or family members to a health problem.[32] If that medication were subsequently found to have side-effects, depending on the dosage, the IoT data would provide proof not only of consumption of the medication but of the dose administered. While old prescriptions or over-the-counter purchase receipts are discarded, the data proving consumption could still exist.

The IoT can also be used by utilities. The 'smart grid' for electricity involves each device on the network being given sensors to gather data (power meters, voltage sensors, fault detectors, etc) and being equipped with two-way digital communication between the device in the field and the utility's network operations centre.[33] In the Kilmore East Bushfire class action in the Supreme Court of Victoria, one of the main allegations concerned the cause of a powerline failing.[34] IoT data may record events causing powerline fatigue and the actions taken by the utility to address powerline failure, which could assist in determining causation.

Similarly, a water network can use devices to ensure the quality of drinking water. Between 1 July and 30 September 1998, increased levels of the parasites Cryptosporidium and Giardia were detected in Sydney's water supply. As a result, Sydney Water Corporation issued a series of 'boil water alerts'.[35] The so-called Sydney Water Crisis of 1998 led to a government inquiry and two class actions. IoT data, in addition to generating real-time measures of water quality to allow for corrective action, may be available to prove the existence of contaminants.

Lastly, the data from wearables such as a Fitbit could provide important information about a person's wellbeing before or after a personal injury. A law firm in Canada sought to use a client's Fitbit history in a personal injury claim. The client was a personal trainer who wanted to show that her activity levels had fallen below baseline

---

30 Kennedy (n 28).

31 Chi Li, 'Maersk — Reinventing the Shipping Industry Using IoT and Blockchain', *HBS Digital Initiative* (online, 28 June 2018).

32 In August 2015, Google and Dexcom (a company that produces continuous glucose monitoring systems) announced plans to produce a dime-sized, cloud-based disposable monitor that communicates the glucose values of diabetes patients in real-time, directly to parents and medical providers: Peter Lefkowitz, 'Making Sense of the Internet of Things' (2015) 59 *Boston Bar Journal* 23, 25. Another example is the GlowCap, a "smart pill-bottle cap" produced by Vitality (and connected to the AT&T mobile broadband network) that contains a wireless chip which can text or phone a patient a reminder if they have forgotten to take their medication. It also has a button that, when pressed, sends a refill request to a person's local pharmacy. See Robin Kester, 'Demystifying the Internet of Things: Industry Impact, Standardization Problem, and Legal Considerations' (2016) 8(1) *Elon Law Review* 205, 211.

33 Greengard (n 27) 70-72.

34 *Matthews v AusNet Electricity Services Pty Ltd* [2014] VSC 663, [75].

35 See PL Stein, "The Great Sydney Water Crisis of 1998" (2000) 123 *Water, Air, and Soil Pollution* 419; Stewart Smith, *The Quality of Sydney's Drinking Water: Current Issues*, NSW Parliamentary Library Research Service, Briefing Paper No. 16/1998.

for someone of her age and profession, and thus, she was entitled to compensation.[36] In a criminal context, Fitbit data has been used against a person as a basis for establishing perjury. The person claimed that they had been sleeping when they were sexually assaulted. However, the Fitbit data showed that the person 'had been awake and walking around the entire night, not sleeping as she had claimed'.[37] In the Federal Circuit Court of Australia, in a matter dealing with parenting arrangements the ESI from a Fitbit worn by a child was unsuccessfully relied upon to demonstrate that the child's sleep problems were linked to contact with the father.[38]

The above examples demonstrate the numerous and wide-ranging situations in which ESI from eObjects may be relevant to a civil dispute. This then necessitates consideration of who or what to approach in order to obtain that ESI.

C *Control of IoT Data*

Obtaining IoT data for litigation requires consideration of the appropriate person or entity from whom to request the data generated by an eObject. This raises in turn issues about ownership of the data and who has access to it. In the Federal Court, standard discovery refers to documents 'that are, or have been, in the party's control'. *Control* is defined in the Dictionary to the rules to mean, in relation to a document, 'possession, custody or power'. *Possession* typically refers to ownership, *custody* to the physical holding of the document (even if there is no ownership) and *power* to an enforceable right to obtain possession.[39]

ESI from an eObject may be within the control of a number of entities. The user of the device, the manufacturer of the device, the retailer/provider of the device, the entity that operates the network, the entity that collects and manages the data produced by the device, or some combination of these may all exercise control. The entities that hold the data, if they become parties to litigation, may be required to provide discovery. Even if not a party, they may be required to produce the ESI through the use of a subpoena. However, a person to whom a subpoena is directed is not required to seek out documents not in the person's own possession and power in order to produce them to the court.[40]

The extent of the obligation imposed in relation to a discovery order and the accessibility of ESI is illustrated by a Victorian decision, *Hanks v Johnston (No 3)*,[41] which dealt with the discovery in a defamation claim of text messages that were thought to have been lost when an Apple iPhone was replaced. Although not addressing IoT as such, Dixon J was satisfied that any iCloud backup of text messages that could be accessed employing particular computer software was within the 'power' of the plaintiff in the relevant sense. Importantly, for the plaintiff to access the backup

---

36 Kate Crawford, 'When Fitbit is the Expert Witness', *The Atlantic* (online, 19 November 2014) <https://www.theatlantic.com/technology/archive/2014/11/when-fitbit-is-the-expert-witness/382936/>.

37 Nicole Chauriye, 'Wearable Devices as Admissible Evidence: Technology is Killing our Opportunities to Lie' (2016) 24(2) *Catholic University Journal of Law and Technology* 495, 509-510.

38 *Oster v Houli* [2015] FCCA 398, [14].

39 Cairns (n 21) [10.140].

40 *Air Pacific Ltd v Transport Workers Union of Australia* (1993) 40 FCR 1.

41 [2016] VSC 629.

data in his iCloud, all that was needed was his user ID and password and the relevant software. Permission or assistance from Apple were not needed in order to gain access.[42] Similarly, ESI from an eObject that a party can access, even if in the cloud, will be discoverable.

In any particular case it will be a matter of fact as to whether a party to the litigation has the power, or not, to access ESI generated from their eObjects. For some eObjects, such as a Fitbit, the owner will be able to download data, as access to the data is part of the functionality that the user requires. However, for ESI from eObjects where access to the data may not be needed, such as the temperatures recorded by a thermostat in determining whether to heat or cool a room, it may not be in the possession, custody or power of the party.

However, even where a party or third party has the requisite control over the ESI, for discovery or a subpoena to be effective the data must be maintained and accessible. An entity may routinely destroy ESI as part of its usual business operations. As a result, a number of further crucial questions arise: what ESI is tracked or stored, and for how long is the data retained? As explained above, some eObjects record on a continuous basis and amass large volumes of data, but as a result that data may not be stored for very long.[43] In others, the data may exist but its preservation may be complicated by issues of cost, burden and contractual obligations.[44]

In *Hanks v Johnston (No 3),* the ability to access ESI depended on it having been retained by Apple in the iCloud, which in turn, depended on both contractual obligations and the operation of the device. Dixon J observed that

> there is uncertainty about the timing of iCloud backups. Automatic iCloud backups occur periodically when the device is screen-locked, connected to a power source and connected to the Internet via a WiFi network. The terms of use state that the last three backups will be stored in the iCloud but space is limited and backup will be subject to other use of the available storage.[45]

Access to ESI created by an eObject may also turn on being able to access the eObject. If the ESI has not been transmitted via the internet to a storage device, such as a server, then the data may have to be downloaded from the eObject. For example, in a US personal injury action by a car driver against the manufacturer of the tyres used on the car, the defendant sought access to the Airbag Control Module ('ACM'). The ACM may have recorded relevant information such as vehicle speed, the driver's braking, and whether the seatbelt was being worn. Usually the data in the ACM is only accessed periodically by a mechanic when the airbag is subject to some form of maintenance. Consequently, the ACM held the relevant data, as it had not been downloaded at the time of the accident. However, the ACM along with the vehicle were not retained by the plaintiff as they were delivered to a salvage yard which destroyed them. In

---

42 *Hanks v Johnston (No 3)* [2016] VSC 629, [34].

43 Ibrar Yaqoob et al, 'Internet of things forensics: Recent advances, taxonomy, requirements, and open challenges' (2019) 92 *Future Generation Computer Systems* 265, 266.

44 Ignatius Grande and Mark Michels, 'The Internet of Things: "You Ain't Seen Nothin' Yet"', *Hughes Hubbard & Reed LLP* (online, October 2014) 11 <https://www.hugheshubbard.com/news/the-internet-of-things-you-aint-seen-nothin-yet>.

45 *Hanks v Johnston (No 3)* [2016] VSC 629, [36].

response, the defendant sought an adverse inference instruction be given to the jury.[46] In this case the judge accepted that the crash investigators would have known that the ACM might have contained important information. However, the concern with both eObjects and the ESI that they generate is that a party may not appreciate that they have relevant 'documents' that are subject to discovery obligations.

In Australia the intentional destruction of documents may result in various sanctions, including dismissal of proceedings, the striking out of a defence or adverse inferences being drawn.[47] However, here the greater concern is with the inadvertent destruction of documents due to a lack of comprehension as to what and how ESI is created by an eObject. In such a situation a party might unwittingly fail to comply with the court orders made in relation to discovery. This would result in the party being in default of a court order, which would then allow further orders such as an award of costs, dismissal of proceedings and the entry of judgment.[48] There is no requirement of 'intentional default or contumelious conduct' for an order to be made, although the circumstances of the default will be important in the Court's weighing of the proper exercise of the discretion conferred by the rule.[49] Contempt orders would also be available, although they are unlikely to be readily made for an inadvertent contravention.[50] Nonetheless, the growth in the existence of ESI from the IoT will impact on a party's preservation obligations.

D *Finding the ESI Needle in the IoT Haystack*

As explained in the introduction, IoT will account for about 10 percent of the data on Earth by 2020. Although courts have sought to limit discovery through altering court rules and actively crafting discovery orders as part of case management, there will clearly be situations where the growth in ESI impacts the discovery process.[51] ESI may be relevant to issues in dispute as argued above, but the volume of data may make finding the relevant data costly and onerous. In particular, the nature of the ESI generated by eObjects as part of the IoT is that a massive amount of data is generated but only a small amount of that data may be relevant to the particular dispute.

The issue may be illustrated by two examples. A six-hour flight on a Boeing 737 from New York to Los Angeles generates 120 terabytes of data that is stored on the plane.[52] Depending on the nature of the dispute only some of the eObjects on the plane and only some of the data recorded may be relevant. Another example is that in 2013 the average household with two teenage children owned 10 internet connected devices, but by 2022 it is estimated the same household will own roughly 50 internet-connected devices.[53] Those devices are eObjects and depending on the dispute may

---

46 *Below v Yokohama Tire Corporation*, 15 CV 529 (WD Wisc, 2017). For an Australian example see Luke Mortimer, 'Tiny data recorder in your car could have big impact', *Daily Mercury* (online, 25 November 2017) <https://www.dailymercury.com.au/news/tiny-data-recorder-in-your-car-could-have-big-impa/3274389/>.

47 See eg *Palavi v Radio 2UE Sydney Pty Ltd* [2011] NSWCA 264, [70]-[71], [93]-[95].

48 *FCR* r 5.22, 5.23, 1.32; *Speedo Holdings BV v Evans (No 2)* [2011] FCA 1227.

49 *Lenijamar Pty Ltd v AGC (Advances) Ltd* (1990) 27 FCR 388.

50 Paul Matthews and Hodge Malek, *Disclosure* (Sweet & Maxwell, 5th ed, 2017) [17.31]-[17.33].

51 *City of Swan v McGraw-Hill Companies Inc* [2014] FCA 1271, [24].

52 Greengard (n 27) 56.

53 OECD, *Building Blocks for Smart Networks - OECD Digital Economy Papers, No. 215* (OECD Publishing, 2013) 4. The report also estimates that by 2022 there will be 14 billion connected devices in the OECD, compared to 1.7 million at the time the report was written.

have generated valuable information, but it will be necessary to determine which devices and which data are relevant, and where the date is stored.

The parties and the courts need to 'navigate a path between providing discovery so as to assist efficient resolution of disputes on the merits, and avoiding discovery abuse that harms parties and other court users' with increased costs and delay.[54] The tools for navigating that path are a combination of court rules, practice notes, active case management, lawyer competence and technology solutions.

Standard discovery in the Federal Court Rules seeks to keep a tight rein on the documents subject to discovery through the combination of direct relevance, reasonable search and party control.[55] Further, the rules allow for 'non-standard and more extensive discovery'[56] where needed.[57] However, all discovery is subject to court control. The increase in ESI generated by the second wave of computing and social media was addressed by the courts via a focus on relevance, necessity and proportionality.[58] The last of these factors may be particularly important in an IoT world. Proportionality is reflected in Federal Court practice notes:

> 10.7 A Request must be proportionate to the nature, size and complexity of the case – ie, the Request should not amount to an unreasonable economic or administrative burden on the Discovery Respondent.
>
> 10.8 If the Court approves a Request, a Discovery Respondent's search for and production of documents pursuant to a Request must be: made in good faith, uninfluenced by any negative impact on the Discovery Respondent (other than legitimate considerations such as genuine legal professional privilege or commercial confidentiality), and should be comprehensive, but proportionate.[59]

A court is required to balance the time, cost and burden of providing discovery of the relevant ESI against the possibility that relevant information will be found.[60] Both defendants and plaintiffs should be encouraged to use proportionality arguments offensively and defensively to control the cost, delay, and burden of overbroad discovery requests.[61] The unrestrained collection and production of IoT data could be 'costly, wasteful, and much of the data could be of little value'.[62] However, for the court and the parties to perform their roles it is essential that they understand the underlying technology and what is involved in accessing the relevant ESI.

---

54 Legg (n 16) 100.
55 *FCR* r 20.14.
56 Ibid r 20.15.
57 Ibid.
58 Chief Justice T F Bathurst, 'Tweeters, Posters and Grammers Beware: Discovery and Social Media Evidence'(Tenth Information Governance and EDiscovery Summit, 21 June 2016) [17], [24].
59 Federal Court of Australia, *Central Practice Note: National Court Framework and Case Management (CPN-1)*, 25 October 2016, [10.7]-[10.8]. See also Federal Court of Australia, *General Practice Note: Technology and the Court*, 25 October 2016, [3.1]-[3.5].
60 *Slick v Westpac Banking Corporation (No 2)* [2006] FCA 1712, [41]-[43].
61 Brian Morris, 'The 2015 Proposals to the Federal Rules of Civil Procedure: Preparing for the Future of Discovery' (2014) 41 *Northern Kentucky Law Review* 133, 147.
62 Christopher Suarez, 'Forensics and Electronic Discovery in an IoT Era', *TYL Magazine* (online, 25 April 2018) <https://www.americanbar.org/groups/young_lawyers/publications/tyl/topics/resources-technology/forensics-and-electronic-discovery-an-iot-era/>.

An important part of the above equation is knowledge of the available technology solutions for accessing and retrieving the relevant data from the eObject or the data storage locations to which the ESI was transmitted. Past experience with technology creating large volumes of data to search, such as with the proliferation of email, was that technology also provided solutions such as technology assisted review ('TAR'), which uses supervised machine learning to rapidly review large volumes of data. TAR reviews written documents that are in electronic form by identifying patterns in the data. The program is provided with a set of documents referred to as a 'seed set' that has been reviewed by a human (lawyer) and labelled as 'relevant, not relevant, privileged, or not privileged'.[63] Using this information, the program codes the documents that may be discoverable. The lawyer reviews a sample of these documents and identifies any errors which are then fed back to the program. This process continues until the program is sufficiently accurate. From the lawyer's seed set and corrections, the software creates 'a predictive model, a kind of profile'[64] of the different types of documents, and this 'mathematical model… can then predict the classifications of other documents in that dataset'.[65] Ultimately, the program generates a probability that a particular item is relevant or not relevant. TAR has been found to be more accurate than human review, as well as quicker and cheaper.

Where the ESI from the IoT is text, then TAR may be able to be employed. However, for many eObjects the ESI may not be words or phrases from human language, but rather numerous measurements of physical characteristics such as temperature, speed or location – in short, numbers. As pointed out above, the function of some eObjects will necessitate easy user access to their ESI. Even commercial uses, such as the Onboard Network System on the Boeing 737 are designed to facilitate ease of access, with the collected ESI being made available to flight, cabin and maintenance teams for both onboard functions and offboard analytics.[66] However, other eObjects like embedded sensors detect changes in environmental factors with a view to facilitating some action, such as turning lights or heating on or off, but the ESI is not readily accessible by the user. In such a situation resort may need to be made to an expert in IoT forensics.

The IoT creates a number of challenges for traditional digital forensics due to the heterogeneous infrastructure of the IoT. Enhanced objects employ diverse proprietary formats. There is limited visibility and a short survival period for the ESI unless it is transferred to some form of data storage. ESI in the IoT environment is spread across multiple platforms including device, communications networks and in the cloud. There is uncertainty as to what, where and how ESI is stored.[67] As a result, research has been undertaken to develop digital forensics techniques, models and methodologies for use in the IoT context. As ESI can reside in multiple locations or

---

63 Matthew Paulbeck, 'The Ethics of Predictive Coding: Transparency and Judgment-Formed Seed Sets' (2017) 30(4) *Georgetown Journal of Legal Ethics* 971, 971.

64 Kevin D Ashley, *Artificial Intelligence and Legal Analytics: New Tools for Law Practice in the Digital Age* (Cambridge University Press, 1st ed, 2017) 241.

65 Shannon Brown, 'Peeking Inside the Black Box: A Preliminary Survey of Technology Assisted Review (TAR) and Predictive Coding Algorithms for Ediscovery' (2016) 21 *Suffolk Journal of Trial & Appellate Advocacy* 221, [2.1] (see generally for a comprehensive technical overview of the TAR process).

66 Victoria Wilk and Tri Phan, '737 MAX Advanced Onboard Network System' (2014) 55 (3) *Boeing Aero Magazine* 5.

67 Maxim Chernyshev et al, 'Internet of Things Forensics – The Need, Process Models, and Open Issues' (2018) 20(3) *IT Professional* 40, 41-42; Yaqoob et al (n 43) 266.

architecture layers, different areas of digital forensics' expertise and tools, such as for smart phones, servers or the cloud, may need to be employed.[68]

The court, the parties and the lawyers will need to weigh what is technically possible and at what cost, with the expected significance of the ESI to the dispute so as to ensure discovery is 'comprehensive, but proportionate'.[69]

E *Lawyer Competence*

A majority of US States have introduced a requirement that lawyers be technologically competent, following a change to the American Bar Association's Model Rule 1.1 in 2012. The Comment to the rule specifies that 'a lawyer should keep abreast of changes in the law and its practice, including the benefits and risks associated with relevant technology'.[70] No such express requirement currently exists in any Australian jurisdiction. However, the Uniform Solicitors Rules provide that lawyers should 'deliver legal services competently, diligently and as promptly as reasonably possible'.[71] For a lawyer dealing with discovery that involves ESI generated by an eObject, competence with technology is necessary to be able to comply with court rules, practice notes and orders. The need for lawyers to have technology competence is illustrated by the Federal Court practice note which states:

> 10.10 Where a Request has been approved by the Court, a Discovery Respondent must, if requested to do so by a Discovery Applicant, provide a brief description of the steps taken by the Discovery Respondent to conduct a good faith proportionate search to locate discoverable documents, such as what records have been searched for, what search criteria or terms have been used, or what databases have been searched.
>
> 10.11 Where a Discovery Respondent asserts that documents are unavailable or burdensome to access and discover, the Discovery Respondent must clarify to the Discovery Applicant (unless there is demonstrably no need to do so), how the Discovery Respondent manages, stores, accesses, destroys and disposes of documents. The Court may require a Discovery Respondent to depose to such information.[72]

The Discovery Respondent will require the assistance of their lawyer to be able to describe how the search to locate documents was undertaken in a good faith and proportionate manner. Further, legal assistance will be part of explaining how documents are managed, stored, accessed and destroyed, especially as the explanation may need to be given to the court.

However, the level of competence required is more difficult to specify in the abstract given the diverse nature of eObjects and the ESI they generate. The lawyer must have a basic understanding of how the underlying technology works, what ESI is created

---

68 Chernyshev et al (n 67) 43-45; Yaqoob et al (n 43) 269-272.

69 *Central Practice Note: National Court Framework and Case Management* (n 59) [10.8].

70 American Bar Association, *Model Rules of Professional Conduct* (2015) Comment 8 to Rule 1.1.

71 *Legal Profession Uniform Law Australian Solicitors' Conduct Rules 2015* (at 1 July 2015) r 4.1.3.

72 *Central Practice Note: National Court Framework and Case Management* (n 59) [10.10]-[10.11]. See also *FCR* rr 20.16, 20.17 which requires a list of documents not searched for or that was in the party's control but no longer is.

and where the ESI may be stored. In addition, the lawyer must comprehend any technology solution such as TAR or IoT forensics to be able to defend what was, or was not found, during the discovery process. However, the lawyer does not need to have the competence of an expert in the area of the IoT or its constituent parts.

F *Privacy and Discovery*

Users of social media who found themselves in litigation were surprised to find that their social media posts or tweets that were relevant to the litigation had to be disclosed and were not able to remain private. Similarly, ESI from an eObject can be required to be disclosed regardless of privacy. Access to private records for litigation recognises the particular position of courts as an arm of the state charged with resolving disputes by reference to evidence to arrive at correct results. For example, in *Lowery v Insurance Australia Ltd*, Basten JA stated that 'the ultimate justification for compulsory production and disclosure of information which might otherwise remain confidential, is the legitimate furtherance of judicial proceedings'.[73]

Yet the courts do have powers and procedures for limiting the disclosure of private information. Where documents or information are required to be disclosed as part of court proceedings, the party obtaining the material cannot, without leave of the court, use it for any purpose other than the litigation, at least until the material is admitted into evidence.[74] Courts are also able to assess the need for privacy or confidentiality by weighing it against open justice, and if the former prevails, making orders to prevent the publication or disclosure of information.[75] The diverse nature of eObjects and the data they collect mandates that careful attention be given to whether private or confidential information may exist in the ESI and requires protection beyond that provided by the 'implied undertaking'.

IoT-derived ESI has been shown to be potentially subject to the court's discovery and subpoena powers as part of the pre-trial steps in civil litigation. The article now turns to examine that ESI in the context of evidence for trial.

IV IOT-DERIVED ELECTRONIC EVIDENCE UNDER THE UNIFORM LAW: HEARSAY

A *Documentary form*

As earlier indicated, we approach our analysis on the premise that the electronic evidence derived from the IoT is to be furnished to the court in documentary form. This premise is not critical to the points we make regarding issues of hearsay and authentication. That is, our points hold if the relevant evidence is to be adduced in electronic form. We take the premise of documentary form because it is the typical

---

73 *Lowery v Insurance Australia Ltd* (2015) 90 NSWLR 320, [10] (Basten JA).

74 *Hearne v Street* (2008) 235 CLR 125, 154-155 [96] (Hayne, Heydon and Crennan JJ). The principle is often referred to as the "implied undertaking" or the "Harman undertaking" after *Harman v Secretary of State for Home Department* [1983] 1 AC 280. It is an obligation of substantive law that applies to the parties to litigation and to third parties, including lawyers, expert witnesses and any other person who comes into possession of the material knowing it to have been obtained by way of court process.

75 See, for example, *Federal Court of Australia Act 1976* (Cth) Pt VAA.

form in which electronic evidence is presented and because it allows our critique of the UEL provisions to be housed against the familiar framework of documentary evidence.

The UEL defines a 'document' as 'any record of information' and inclusively provides for 'anything on which there is writing', 'anything on which there are marks, figures, symbols or perforations having a meaning for persons qualified to interpret them' and 'anything from which sounds, images or writings can be reproduced with or without the aid of anything else'.[76] This definition, no doubt, includes ESI.[77]

The contents of a document, including an electronic record or data, may be admitted into evidence through the tender of that document or one of a number of alternative means specified in s 48 of the UEL, including tendering a copy of the evidence or:

> if the document in question is an article or thing on or in which information is stored in such a way that it cannot be used by the court unless a device is used to retrieve, produce or collate it—tendering a document that was or purports to have been produced by use of the device.[78]

In *Wade v DPP*,[79] it was held that closed circuit television footage is clearly a document capable of reproduction using an appropriate device to reproduce the images.[80] By analogy, data may be converted by a device with the appropriate software into a comprehensible format and therefore may be admitted through s 48(1)(d) of the UEL. The data extraction and transformation process may need to be supported by the expert testimony of the forensic computer technician who performed the work. The Australian Law Reform Commission explained that the purpose behind this provision is to enable admission of secondary evidence of the contents of modern information storage media and, in particular, data and electronic information in a comprehensible form, such as through a printout or via the display of the information using software.[81]

A party wishing to adduce evidence of the contents of a computer record may do so by way of a hard copy document, including by tendering the printout of some electronic file where appropriate.[82] The abolition of the 'best evidence rule' conveniently allows electronic evidence to be tendered absent debate over originality, as the concept of and distinction between 'copy' and 'original' is not a straightforward one.[83] The simplicity and feasibility of doing so depends on the nature of the data or electronic record to be adduced; a digital photograph can be easily printed or displayed in a graphic form, whereas some gathered data, such as the geolocation data from a fitness tracker, may not so easily be reproduced without active data processing and presentation.

---

76 UEL s 3 (definition of 'document').

77 See, for example, *Sony Music Entertainment (Australia) Ltd v University of Tasmania* (2003) 129 FCR 472.

78 UEL s 48.

79 (2014) 41 VR 434

80 Ibid [24].

81 Australian Law Reform Commission, *Evidence (Interim)* (Report No 26, 1985) vol 1, 26 [651]; see also Stephen Odgers, *Uniform Evidence Law* (Thomson Reuters, 13th ed , 2018) 272.

82 Justice Peter Brereton, 'Evidence In Civil Proceedings: An Australian Perspective On Documentary And Electronic Evidence' (Speech, National Judges College of the Supreme People's Court of The People's Republic of China, September 2007).

83 Allison Rebecca Stanfield, 'The Authentication of Electronic Evidence' (Doctoral Thesis, Queensland University of Technology, 2016) 12.

B *Previous representation made by a person*

Relevant documentary evidence without an original use is hearsay. Documents are traditionally scribed by a person and vulnerable to inaccuracy. Acknowledging the raft of exceptions that are tantamount to hearsay being a rule of re-inclusion, the UEL hearsay rule purports to prevent unreliable evidence of intended previous representations by precluding the admission of representations which cannot be challenged for meaning.[84] Section 59 acknowledges the fallibility of representations made by people, whether that be a result of a self-held or pressured motive to record untruths, poor recollection, or an inability to recall with precision. Traditional documentary evidence may contain representations of fact adduced to prove the truth of those facts. The introduction of autonomous data-generating technology, such as that integrated into eObjects, has introduced a new species of documentary evidence that is, arguably, not subject to the perils of paper documents prepared by humans.[85]

IoT-derived evidence is not directly generated by a person. It is produced as a result of encoding written by a human, but assuming the verifiable and proper function of that code, the IoT evidence objectively records in accordance with the code. It is unaffected, at the point of its ambient recording, by human error, bias or motivations; again, other than those deliberately or unwittingly forming part of the program as a result of the originating source code of the eObject.[86] Some familiar territory that cross examination would demand be traversed in respect of such statements, hence the application of the hearsay rule, need not be trodden in the case of ESI produced from the proper function of an eObject. Concerns about recollection, dishonesty, deceitfulness and fabrication, interpretation of information, understanding of events or observations, bias or prejudice, details lost in transmission and the dangers of inaccuracy in repetition[87] are averted in the absence of human involvement in the generation of the electronic evidence distilled as a document.

This evaluation rests on the rationale of the hearsay rule restricting it to representations made by persons. Section 59(1) of the UEL provides:

> (1) Evidence of a previous representation made by a person is not admissible to prove the existence of a fact that it can reasonably be supposed that the person intended to assert by the representation.

The electronic evidence derived from IoT that is adduced to prove facts asserted by its representations may be regarded as exempt from the hearsay rule depending on the scope of 'made' for the purposes of s 59.

The compilation of ESI that is wholly generated by the operation of an eObject can be regarded as outside hearsay and need not be subject to any exceptional admission

---

84 UEL, s 59.

85 See discussion below concerning 'black box' issues and the analogous concerns relating uniquely to electronic evidence.

86 In a related context, see, Peter B Imrey and A Philip Dawid, 'A Commentary on Statistical Assessment of Violence Recidivism Risk' (2015) 2(1) *Statistics and Public Policy* 25.

87 Australian Law Reform Commission, *Uniform Evidence Law* (Report No 102, February 2006), [7], [7.9].

requirement.[88] To what extent can second and third category generations of electronic evidence, as we have outlined those categories, be regarded as not 'made' by a person?

C *Passively-generated representations*

Second and third category eObjects record data, which would constitute previous representations for the purpose of s 59 if later reduced to tangible output in the form of documentary evidence, without direct command or instruction from a person for that data to be recorded.

Second category eObjects require a direct computer-human interaction. Examples of these eObjects include a car that gathers, records and transmits data about automotive performance and geolocation, or an electric toothbrush that tracks and transmits data on battery life and usage. These devices record data (representations) as a result of their operation by a person. Those representations are not however, commanded, instructed or the result of the person directing the eObject to produce a particular record. The data is causally created by human operation of the eObject but the causative effect is with respect to the eObject operating – the human does not cause any particular data to be recorded. The recording of the data is a consequence of the operation of the eObject. The content of the data recorded is caused by the source code of the eObject, which operates by derivative rather than direct result of the usage of the eObject by a person. To illustrate using a non-technological example: Person A sets fire to a house in the view of Person B. Person B shouts "fire, fire!". A feat of Romanian gymnastics is required with the meaning of causation to allow a conclusion that A has made B make the representation of "fire, fire!" The representation of B derived from what A did, but the representation was made by B, it was not made by A. Absent a direct input from a person to produce a particular data set, such that the technology may be regarded as a mere medium (ie the sending of texts or emails) it is difficult to conclude that that data is made by a person.

It might be argued that the operation of second category eObjects results in the person indirectly making the representations recorded as data. This would capture the recording of data by eObjects where that data was recorded as a derivative result of the operation of the eObject by a person. That approach would require the meaning of 'made' in s 59(1) to include representations directly or indirectly made by a person. Where direct or indirect inference or cause is pertinent to the test, the UEL provides for that language, 'direct or indirect' to be expressly stated (see, eg, s 55). In the absence of such language, indirect causation can be regarded as outside the scope of 'made' for the purposes of s 59(1). This position against indirect scope of the provision is supported by the restriction of the hearsay prohibition to intentional, as opposed to unintentional, assertions.

Third category eObjects are more readily detached from human input. These eObjects, as we have defined, record data according to programming that is built into the autonomous function of the device. Provided there is power to the device and it is 'on', the device records data regarding ambient conditions irrespective of any human input, indeed, for as long as the power is connected. Persons may affect the recording of a third category eObject. For example, leaving the windows open or closed will affect air

---

88 See the reasoning in decisions such as *Mehesz v Redman (No 2)* (1980) 26 SASR 244, 252 concerning computer analysis and record generation.

control temperature readings on air conditioners, as will the number of foodstuffs placed in a refrigerator. These human activities, however, could not be regarded as sufficiently proximate to the data recorded by the eObject such that they 'make' the representations.

It appears that the greater the automation of the technological (eObject) device, and the more passive the human input, the more irrefutable it is that the data recorded will not be subject to hearsay restriction, to the extent that the data provides relevant representations.[89] The inapplicability of a fundamental evidential safeguard against unreliable evidence, the hearsay rule, to a burgeoning source of evidence, namely third wave technology, should be of concern. The bases of those concerns may be centred around the difficulties inherent in authentication of IoT-derived electronic evidence.

An example introduces the problem. Revert to the exemption of third category eObjects from the hearsay rule as recording representations not made by persons. That presumes persons were passive with respect to the source data from which the eObject records. As observed in describing the three categories, the third category (just as the second) may be overridden by direct human input. Taking actions to deliberately increase the temperature of a room or appliance will, of course, alter the data autonomously recorded by the sensory capacities of the eObject. In that case, the present answer on the hearsay prohibition may be turned around: the data recorded by the eObject reflects representations that may be attributed to a person and regarded as being made by them. If Person A lights the fire and then threatens to harm Person B unless Person B yells, "fire, fire!" it can far more readily be concluded that the representation was made by Person A, at least causatively. Similarly, if a room is heated or cooled, the person doing that may be regarded as making the representations of high or low temperatures the eObject in the air conditioner records. The point is that in these examples, as a matter of principle, the hearsay rule has work to do because the ambivalence of technology which grounds our exclusion of its data from the rationale of hearsay, is replaced with an appreciation that the eObject, like Person B, has been the vehicle for the making of representations of another person. The response to all this may be, of course, that it is a matter of evidence in each case as to whether admissibility rules will apply. The retort to that tautologous criticism is how will we know or detect if the autonomously operating eObject has been altered or manipulated?

V IOT-DERIVED ELECTRONIC EVIDENCE UNDER THE UNIFORM LAW: AUTHENTICATION

A *The Humanity of Authentication*

The authentication of evidence traditionally introduces two critical aspects of evidence to the court: its identity and its provenance. Doctrinally, authentication requires that a party adducing evidence prove that the evidence is what the party claims it to be, by identifying what it is, its authorship, its provenance, the chain of custody or possession and, in the case of electronic evidence, the proper functioning of the device that generated the evidence. In the case of documentary evidence, authentication is

89 Odgers (n 81) 364-5.

typically via the testimonial evidence of the author of or someone with personal knowledge about the document.[90]

How is ESI produced from an eObject within the IoT authenticated? The inclination would be to treat IoT-derived evidence like any other electronic evidence. It looks the same as other pre-third wave evidence when presented to court – it is being adduced as a document. The provenance may also be neatly explained as a print out from the relevant device, for example, a FitBit device. But, if IoT-derived electronic evidence has been changed, deliberately or accidentally as discussed earlier, its very authenticity is called into question in a manner that may not be addressed, in like fashion to situations where manipulation concerns involve non-electronic-derived or first category electronic-derived forms of real evidence. The critical difference is the absence of human input in the ordinary functioning of the device.

The absence of human input denies the traditional, ubiquitous means by which courts sought to establish the authenticity of evidence and give confidence and credence to their decisions regarding real evidence – namely, human testimony. In 1999, Bryson J enumerated the traditional bases on which the authenticity of evidence was established, all of which relied on human input. His Honour said:

> …the authenticity of a document may be proved by the evidence of the person who made it or one of the persons who made it, or a person who was present when it was made, or in the case of a business record, a person who participates in the conduct of the business and compiled the document, or found it among the business's records, or can recognise it as one of the records of the business.[91]

Bryson J laid emphasis to the essentiality of human input into the determination of authentication. He said:

> The Court acts almost always on narrations which must have a human origin…For the Court to feel confident that it should act on any narration it is very important to have a human witness who has pledged, by oath or affirmation, that the narration is true: someone who is responsible for it.[92]

In the context of electronic evidence, this requires the party to prove that the evidence is what it purports to be, requiring that its identity, manner of generation, origin, provenance and handling history are proved. In relation to traditional, first category computer-generated evidence, denoted by active human input, this required that the proper or ordinary function of the computer or device, at the time the evidence was generated, be addressed.[93] Authentication could, in most cases, be achieved through the admission of an affidavit by a person who, at the time when the evidence was generated or afterward, had responsibility for the creation or keeping of the evidence.[94]

On this, the 20th anniversary of these remarks, the courts are faced with a dramatically increased, and increasing, amount of electronic evidence. The third wave challenge of

---

90 Cf the position in the USA, in which metadata has been used as a means to authenticate electronic evidence: *Lorraine v Markel* 241 FRD 534 (D. MD, 2007).

91 *National Australia Bank Ltd v Rusu* (1999) 47 NSWLR 309 (‘*Rusu*’), [17].

92 Ibid [34].

93 Odgers (n 81) 349.

94 UEL ss 170, 171.

electronic evidence is the removal of human input from the operation of the technology capturing the electronic evidence. Previous technology produced outputs which, whilst calculated and compiled by machine, did so at points in time which were set and commanded by human input. This provided for a human connectivity to the chronology of the generation of electronic evidence. Autonomous recording, storage and transfer removes human direction or oversight of the data. Accessing IoT-derived electronic evidence is a distillation of intangible evidence, the recording of which may not have been commanded or visited by a human being until the point of download. Autonomous computing relocates the human element to a retrospective point of access, where previous waves of computing required point of capture by human input.

The absence of human input removes the IoT-derived evidence from the purview of the hearsay rule because the automation of recording eliminates the potential human foibles and infractions against which hearsay guards. The paradox is that this pathway to admissible use relies on the very divorce of the IoT from human input, monitoring or awareness that derogates from the capacity of the human-centric trial to authenticate IoT-derived electronic evidence. This derogation is likely to become more significant as future waves of autonomous technology decreasingly rely on human input; whilst humans increasingly rely on these technologies.

The automatic paradox in litigation is consistent with, and an extension of the general, or workforce, automation paradox.[95] The workforce paradox finds the need for human labour contributions increases as automation of workforce tasks increases; even if the human contributions required are different in type from previous labour tasks, which have been tasked to technology. The paradox is that the increase in automated tasking does not decrease the need for human tasking. This is consistent with the automation paradox in litigation which depends on human input to authenticate outputs of autonomous technology. The workforce paradox sees the increasing need for human input to perform tasks derivative from increased automation. The litigation paradox shares the same quality of requiring human input when the autonomous operation of the technology should seemingly suggest the capitulation of human involvement.

The unique problems in authenticating IoT-derived evidence may be illustrated by comparison to authenticating traditional forms of real evidence. Take, for example,[96] the knife produced by the Crown on a violence charge where it is said to be the relevant weapon. If the knife is shown to have been collected from the scene, there is a prima facie basis for its authentication. If counter arguments suggest the knife has not been kept according to chain of custody rules, has been altered, or has otherwise been the subject of tampering, the court may exclude the knife from evidence altogether as not being the evidence it purports to be (which may result in the *nolle prosequi* of the prosecution case). It is more likely that this contest will be left to the course of trial and affect the weight to be accorded the knife as a piece of evidence. We note that the point at which authentication arises for consideration is unsettled. One line of authority suggests it is a pre-condition to admissibility, another line of authority indicates it is a matter for the tribunal of fact going to the weight of the evidence. We discuss this below. Presently, the point is that, regardless of the line of authority followed, the

---

95 See, eg, James Bessen, 'The Automation Paradox', *The Atlantic* (online, January 19 2016) <https://www.theatlantic.com/business/archive/2016/01/automation-paradox/424437/>.

96 Noting that while an example from the criminal trial perspective has been selected as particularly memorable, the same principles apply in the civil trial context.

authentication of the knife is an argument that is within the structure of the UEL and the tenets of the adversarial trial to resolve because its provenance is almost certainly a contest of human testimony.

Take, for further example, the document in a civil dispute that the plaintiff claims to be genuine and the defendant claims to be forged. Support for their respective arguments may involve allegations that certain machines were used to produce a signature; they may rely on expert evidence regarding technological processes that could have imitated a signature. The reliance on technology in these supposed contentions still locates the use of technology as an extension of direct human input. Whether technological devices were used to produce the signature, just as in cases where the claim is forged handwriting, the evidence regarding the contentions is dependent on human input and direct human involvement.

In the case of second and third category eObjects forming the IoT, the human input is absent. The ESI is reduced to a tangible form at a later point in time than its capture. The human who downloaded and produced (printed) the data may be able to speak to that process, but for IoT-derived evidence the point of capture, storage and network transfers have all occurred without human command, or even awareness. In the inverse situation, where deliberate manipulation is involved, the autonomous eObject is not able to produce a record or metadata that would indicate any particular interference.

The circumstances in which electronic evidence derived from eObjects may be susceptible to undetected and even undetectable (depending on the self-diagnostic programs and capacity of the eObject) alteration are increased from earlier, immobile technology. The mobility of eObjects, and the consequential volatility and vulnerability that result, provides a myriad of circumstances in which their initial or transferred capture of data could be changed. We outline a non-exhaustive list.

First, electronic evidence is liable to be unalterably and untraceably manipulated, intercepted and/or modified. This is especially for eObjects which by virtue of their mobility frequently transmit over networks that may be private or public with different security protocols in place. Security concerns may be divided into two deliberate forms: those relating to human or automated cyber-attack on the IoT, and those relating to physical (real-world) intervention with a data storage medium. In the latter case, signs of interference may be more readily detectable but the effect of that interference on intangible electronic data may remain inscrutable.

Secondly, electronic evidence from eObjects may be similarly altered by inadvertent or accidental actions. For example, placing cold or hot objects, insulation or conducting materials around eObjects taking temperature readings may manipulate the data in unintended ways. Whilst these extrinsic matters could themselves be the subject of evidence, akin to whether an eyewitness is wearing prescribed spectacles, in the case of electronic evidence the occurrence or otherwise of the extrinsic matters affects the output electronic evidence such that uncertainty arises with respect to whether it is what it purports to be. The same is not true of tangible forms of evidence that human sensory capacity (sight, for most evidence) can adjudge as at least meeting the threshold provenance requirement of authentication.

Thirdly, electronic evidence may mislead or misrepresent on account of ineffectual or intermittent use by humans. For example, a motion sensor may be incorrectly orientated towards a nearby wall or closed area rather than toward an open area that it ostensibly monitors, resulting in data that may misrepresent activity in the open space. Similarly, a wearable fitness tracker may be worn at some times and not others, or may be worn by several persons at various times. Absent testimony, these differentiations may be inscrutable and, in such a case, the authenticity of the electronic evidence is linked to human testimony in such a way that there is no independent basis for the electronic evidence to assert its own provenance. This is contrary to the general approach to machine generated evidence as being what it purports to be.

Finally, eObject-derived electronic evidence must be stored and extracted, and may need to be processed, in order to be presented in a comprehensible form as evidence. The integrity of each of these processes is vital to ensuring the tangible form purports the intangible form, and each process is susceptible.

ESI is unique, in the sense that the intangible data, being information itself, is evidence, as opposed to some tangible storage medium containing the information. The authenticity of the digital media must be examined by reference to the information itself. It has been suggested that the identity of the information (that is, what it purports to be) and its constancy (that is, that it has not been altered or modified without a precise record of that alteration or modification) are the key characteristics of authenticity and the notions of 'immutability' or 'integrity' encompassed by authentication.[97] The integrity of electronic evidence depends largely on the authorship and authenticity of the enabling technology. This traditionally depended on the proper operation of the device that created the ESI, and required that the electronic record had been extracted and handled without altering or omitting any information.[98] The authenticity of the evidence, in particular, is determined by whether the ESI has been altered or modified since its creation (and whether any such modification has been recorded precisely).[99]

Electronic evidence must be what it purports to be. No matter where this task is assigned in the trial process, discussed below, it is made difficult on account of electronic evidence being a reduction of the intangible to the tangible. This reduction has been problematic for all generations of technology-derived evidence, including the traditional non-autonomous technologies dependent on human input. Determining the origin, provenance and vulnerability to contamination of data generated and transmitted by IoT linked eObjects is especially challenging, given the absence of human input, and so therefore are the resulting lacunae that can arise in testimony of commands, chronology and visual confirmation regarding data.

---

97 George L. Paul, *Foundations of Digital Evidence* (American Bar Association, 1st ed, 2008), 36.

98 See Stanfield (n 83) 11; see also Yatan Dahiya and Sunita Sangwan, 'Developing and Enhancing the Security of Digital Evidence Bag' (2014) 1(2) *International Journal of Research Studies in Computer Science and Engineering* 14-25. See also Paul (n 95) 15ff.

99 Stanfield (n 83) 11.

B *Traditional authentication*

It has been suggested that the court will use two criteria to measure the weight of electronic evidence. One, probative value, which takes heed of the authorship, authenticity, correct operation of a device and reliability of the evidence (and the device that generated it). Two, whether the evidence has been properly extracted and handled (and if necessary, transformed into comprehensible format).[100] The authenticity of electronic evidence may be disputed through challenging the provenance and historic handling of the ESI. Challenges focus on exposing uncertainties over how the electronic evidence came into existence and its treatment since then, including any transformations, alterations or adulterations. Examples include: scrutiny over the identity of the operator of the relevant device; scrutiny over the reliability of the relevant computer software; a claim that the ESI was altered, manipulated or damaged between the creation of the ESI and the commencement of proceedings; or a claim that the ESI was altered, manipulated or damaged when it was extracted for the purpose of the proceedings.[101]

We have outlined the significance of the authentication problem for IoT-derived electronic evidence compared with traditional approaches to authentication of tangible and human input-derived computer evidence. We explained the particular authentication points for ESI derived from eObjects in consequence of outlining how the mobility of many eObjects promotes authentication issues arising from their volatility and vulnerability. The uniform law nonetheless provides that evidence is admissible if it is 'relevant in [the] proceeding' and is not excluded by provisions of the UEL.[102] Evidence is relevant where 'if it were accepted, [it] could rationally affect (directly or indirectly) the assessment of the probability of the existence of a fact in issue in the proceeding'.[103]

The law is unsettled with respect to whether challenges to authentication are matters of law or matters of fact under the UEL. If they are the former, they rightly arise for the tribunal of law to determine in consideration of the admissibility of evidence. This view was espoused by Bryson J in the New South Wales Supreme Court.[104] If authentication is not a question going to admissibility but rather a matter left to determinations of fact and assessments of the probative value of evidence, questions of authentication do not independently arise in determining admissibility and are matters of fact to be left to the tribunal of fact. This view was advanced by Perram J in the Federal Court,[105] in rejection of the Bryson J view. The relevant debate is about whether a challenge to the authenticity of evidence is a question of law, for the tribunal of law to determine as a prerequisite to admissibility and as a separate and independent question from that of relevance, or, whether it is a question of fact such that authentication does not arise as a requirement of admissibility. The outcome of that debate ultimately pertains to who should determine an authentication question and at which point/s of trial. That outcome does not, and does not purport to, address how challenges to authentication can be adequately resolved given the significance and

---

100 Stanfield (n 83) 11; see also Dahiya and Sangwan (n 96) 14-25; see also Paul (n 95) 36.
101 Stanfield (n 83) 187.
102 UEL s 56.
103 UEL s 55(1).
104 *Rusu*.
105 *Australian Competition and Consumer Commission v Air New Zealand Limited (No 1)* [2012] FCA 1355 ('*Air NZ*').

novelty of authentication issues that can arise with respect to electronic evidence deriving from eObjects in the IoT.

In circumstances where data is generated by a device or computer, it is possible that no such person is available, or exists, to provide that testimonial evidence. For data generated while an eObject is being used or operated by a human, the human can give evidence about the use or operation of the device but not about the data generated concurrently by the device. For evidence generated autonomously by the ordinary independent operation of the eObject, an expert may provide evidence on the processes by which the ESI was generated, as was recently the case in Canada in respect of data extracted from a wearable fitness tracker.[106] The expert however, is limited to testimony of the same type as given for first category technology – testimony regarding ordinary process and function. It has been suggested that the authentication of electronic evidence is a 'trivial showing' and a formality subordinate to the substantive interrogation of the proper function of the system, software or device that generated the evidence.[107] Conventionally, the admissibility of electronic evidence has been determined by the question of whether the device that generated the evidence was functioning correctly, or as it would be expected to operate, at the time the evidence was generated.

This inquiry is facilitated by the presumptions contained in ss 146 and 147 of the UEL, which are rebuttable upon furnishing evidence that the device malfunctioned or functioned in an unexpected way when generating the evidence. The operation and significance of these provisions is discussed later. The ESI gathered by action of eObjects in passivity of human input defies human sensitivity or awareness of its timing and manner of collection. Electronic evidence is typically authenticated by methods which are limited to analysis of computer coding to determine if the machine functions according to its code. Putting aside issues regarding the accessibility of that code,[108] and assuming the code is verifiable, the examples we have given earlier indicate that the proper functioning of the technology can be an incomplete answer to the authenticity of the electronic evidence produced. This owes to the reduction of the intangible to the tangible and the absence of human activity in the point of information collection, which would otherwise serve as a check and balance.

The authentication problem for IoT-derived evidence is that of knowing what we are accepting. Returning to earlier examples, even if a dispute arises, we know the knife is a knife, even if there is a problem in its handling; we know the forged document is a document disclosing some contract or bequest, even if it does so fraudulently. How do you authenticate something the provenance of which is not traceable to the time of its creation but only the time of its output? What is the reference point? Whether it is a legal or factual criterion, the question is: what is being prima facie accepted?

---

106 Parmy Olsen, 'Fitbit Data Now Being Used in the Courtroom', *Forbes* (online, 16 November 2014) <https://www.forbes.com/sites/parmyolson/2014/11/16/fitbit-data-court-room-personal-injury-claim/#762ecff97379>.

107 Stanfield (n 83)12.

108 See, eg, Imwinkelried (n 15) 97.

C *Unknowing acceptance*

The following example illustrates the point. We first frame the example using output from a first category device, a mobile phone. The example is true and, as will be apparent, may be familiar. Person X flies from Sydney to Paris. Upon landing in Paris, X turns off 'flight mode' on their smartphone and takes a photo from the plane window of a 'Welcome to Paris' sign affixed to the terminal building. Person X returns the phone to their pocket, disembarks, collects baggage and departs for their hotel. Following a rest, X retrieves their phone and sends the photo via MMS to a friend at home, in Sydney. The friend replies by text, 'that is an odd sign to see in Sydney…' Person X, momentarily confused, looks again at the photo just sent and now observes it is geotagged and time-stamped as taken in Sydney, Australia at 22.03 (22.05 was the departure time of the flight from Sydney to Paris and it was close to if not at this time that X recalls switching the phone to 'flight mode'). Unrecognised and unknown to X, at the time of taking the photograph aboard the landed plane, the phone's settings had not updated, given the switch from flight mode and the change of continent, and the photo was logged with a Sydney geolocation and Australian timestamp.

Consider if this photo was to be adduced in court proceedings to establish place or time of its generation by X, or any other matter referrable to its recording of time and place. In our example, of course, there would be evidence to negate the authenticity of the photograph as being taken at the time and place recorded. There is the visual content of the photo itself ('Welcome to Paris'); the associated response from the friend expressing surprise; the flight itinerary showing X had a booked flight to Paris and the evidence of Person X indicating the circumstances in which the photograph was taken. Authentication is often established through testimonial evidence but can also be shown through circumstantial evidence. All this evidence permits of a finding, in contradiction of the metadata of time and place, that the photo is not authentic, that is, it is not a photo taken in Sydney at 22.03 local time, as it purports. The point however, is that that finding is entirely dependent on evidence directly from or deriving from human oversight and input into the making of the photo.

Assume the photo had not included the welcome sign. Rather, the eager tourist X had simply taken a 'touchdown photo' of the runway and other nondescript surrounds. There would be no visual alert in the output photo to query the authenticity of the metadata for the photo; it could be a runway in Australia. Assume the photo was not sent by X to a friend, but that X simply took the photo for posterity. Assume X does not look at the photo until some distant time in the future, months or years, in chance reminiscing. The human input that could indicate the dubious provenance of the photo would not exist or, likely, be significantly eroded by memory. There would not be anything revealed by the metadata itself, or the encoding of the photo feature of the smartphone, to suggest error with respect to the metadata. In the United Kingdom and the United States, metadata accompanying files has been successfully employed as a means of authenticating ESI.[109] More importantly, why would the metadata be checked in the first place? For instance, the photo could be shown as not taken in Sydney by certified photos of runways in Sydney airport, but why would such a survey of airports be undertaken? The photo, retrieved at a point sometime after its creation, would appear in all respects as it purports, a photo taken in Sydney at the recorded

---

109 *Greene v Associated Newspapers* [2005] QB 972; *Lorraine v Markel* (2007) 241 FRD 534, [15] – [16].

time, and there would be a dearth of material to suspect, let alone from which reasonable inferences could point,[110] to the contrary.

In the modified example, there would be little if anything from the photo itself, its associated metadata or the smartphone device to suggest it was other than a photo taken in Sydney. This is possible in situations where the electronic evidence is produced by first category technology that remains controlled by active human input. The potential for second and third category technology, passive eObjects, to record erroneous data is palpable given their recording of information at times and places autonomously from human awareness or command. The advent and proliferation of autonomous technology demonstrate the difficulty in forcing their authentication into traditional approaches that rely on the tangible form of the evidence and the safeguard of human input.

D *Determining authenticity*

As we have discussed, the admissibility of electronic evidence is often dealt with by reference to whether the device functioned properly at the time the evidence was generated. The rebuttable presumptions contained in ss 146 and 147 of the UEL are relevant to the inquiry. Section 146 provides that:

> (1) This section applies to a document or thing:
> (a) that is produced wholly or partly by a device or process; and
> (b) that is tendered by a party who asserts that, in producing the document or thing, the device or process has produced a particular outcome.
>
> (2) If it is reasonably open to find that the device or process is one that, or is of a kind that, if properly used, ordinarily produces that outcome, it is presumed (unless evidence sufficient to raise doubt about the presumption is adduced) that, in producing the document or thing on the occasion in question, the device or process produced that outcome.

Section 147 provides a similar presumption for documents (only) in the context of the production of business records (applying a similar test to the business records hearsay exception).

The presumption in s 146 of the UEL relates to documents (which itself is broadly defined) and 'things'. In *North Sydney Leagues' Club Ltd v Synergy Protection Pty Ltd*,[111] Beazley JA, with whom MacFarlan and Whealy JJA agreed, said:

> Section 146… does not declare the presumed fact to be the fact. Rather, the Court first needs to be satisfied, viz '[i]f it is reasonably open to find' that the device is of a certain kind and performs a certain function before the presumption operates. The presumption will not arise if there is evidence that raises a doubt about the presumption. Evidence that raises 'a doubt' does not need to be of the same quality or of the same probative strength as evidence that is required to satisfy the civil standard.[112]

---

110 See UEL s 58.

111 (2012) 83 NSWLR 710.

112 (2012) 83 NSWLR 710, [60]; see also Odgers (n 81) 1287; Australian Law Reform Commission, *Evidence (Interim)*, (Report No 26, 1985) vol 1, 26 [705].

The presumption weighs in favour of evidence generated by technology being generally reliable and trustworthy and eliminates the need to prove the working accuracy or proper function of the device. The primary issue addressed by the provision is the inefficiency in proving the provenance, accuracy and genuineness of every photocopy, copied media storage device, tape recording or other form of evidence produced in the normal course of a device's operation. Of course, the presumption is rebuttable by evidence sufficient to raise doubt about the proper operation of the relevant device. That evidence need not meet the same quality as would be required under the civil standard of proof. A party opposing the admission of the evidence bears the burden of furnishing sufficient evidence that the document has been produced by the device in accordance with the usual functioning and output of that device. While the burden of proof shifts, by operation of the statutory presumption, the party opposing the admission of the evidence need only provide sufficient evidence to raise doubt. This, says the court, is a substantially less onerous burden than the civil standard,[113] in that the party need not prove that the contrary is true.

Section 56 of the *Evidence Act 1929* (SA) now provides a like test to that of the UEL, although the South Australian provision removes any probabilistic comparison as it only requires 'evidence to the contrary' of the presumptive positions to displace the presumption. The previous, now repealed, s 59B of the South Australian evidence law provided for the following incremented test:

> (1) Subject to this section, computer output shall be admissible as evidence in any civil or criminal proceedings.
> (2) The court must be satisfied—
>
> (a) that the computer is correctly programmed and regularly used to produce output of the same kind as that tendered in evidence pursuant to this section; and
> (b) that the data from which the output is produced by the computer is systematically prepared upon the basis of information that would normally be acceptable in a court of law as evidence of the statements or representations contained in or constituted by the output; and
> (c) that, in the case of the output tendered in evidence, there is, upon the evidence before the court, no reasonable cause to suspect any departure from the system, or any error in the preparation of the data; and
> (d) that the computer has not, during a period extending from the time of the introduction of the data to that of the production of the output, been subject to a malfunction that might reasonably be expected to affect the accuracy of the output; and
> (e) that during that period there have been no alterations to the mechanism or processes of the computer that might reasonably be expected adversely to affect the accuracy of the output; and
> (f) that records have been kept by a responsible person in charge of the computer of alterations to the mechanism and processes of the computer during that period; and
> (g) that there is no reasonable cause to believe that the accuracy or validity of the output has been adversely affected by the use of any improper process or procedure or by inadequate safeguards in the use of the computer.

---

113 Odgers (n 81) 1286; *North Sydney Leagues' Club Ltd v Synergy Protection Pty Ltd* (2012) 83 NSWLR 710, [60].

The factors listed are a 'checklist' concerning the production, storage and communication of ESI that are relevant to its reliability and provenance. The factors remain based on authentication of machine output being human-centric. As technology records, stores and transfers data independent of human input or monitoring, these legal provisions, regardless of their extent and descriptiveness, become decreasingly fit for purpose because the questions they are asking and the inquiries they permit to be made will decreasingly reveal any basis to query or doubt the operation and output of the autonomous technology. Enhanced objects connected to the IoT are part of a networked autonomous evidence gathering system which, excluding the provision of power supply, remains largely and increasingly uninterrupted or commanded by human input. The notable involvement of human input is to retrieve prior recorded and stored data.

E *The adequacy of authentication provisions*

The presumptions concerning both the admissibility and the authenticity of computer-generated evidence in the UEL do not expressly address (a) the security around the device that generated the relevant data, (b) security over the data during transmission and in storage, (c) the authenticity of the ESI itself, as opposed to the reliability and authenticity of the process or device that generated it.[114]

Issues (a) and (b) are of particular concern, as data is, once obtained, so easily and irreversibly modified, often with little trace of the alteration if the alteration is affected by an expert hand, without the author or user of that data being aware of the alteration. This is particularly the case in circumstances where an eObject is connected to a network such as the internet, and data can be intercepted and modified intra or post transmission. In a submission to the Australian Law Reform Commission, the Law Society of New South Wales submitted that s 146 envisages application to machine-produced evidence such as photocopies and other simple processes, which are not applicable to far more sophisticated processes such as the generation of data by computers, especially in light of the facts that such data can be affected by 'bugs' and inherent software infirmities, or may be carefully and untraceably manipulated and accessed by powerful viruses and hackers.[115]

Issue (c) appears to have been addressed in Canada through the imposition of the following burden on a party seeking to adduce electronic evidence:[116]

> [T]he person seeking to introduce an electronic record [in any legal proceeding] has the burden of proving its authenticity by evidence capable of supporting a finding that the electronic record is what the person claims it to be.

This places the emphasis on proving the identity and integrity of the ESI itself, as opposed to the system that generated it, although whether this is practically achieved is doubted by some proponents.[117] The provision performs the task of allocating

---

114 See Stanfield (n 83) 38; see also Emmanuel Laryea, 'The Evidential Status of Electronic Data' (1999) 3 *National Law Review* 1 [27].

115 Litigation Law and Practice Committee of the Law Society of New South Wales, Submission E 103, 22 September 2005, 173; Stanfield (n 83)192.

116 *Uniform Electronic Evidence Act* (1998) (Can) s 3.

117 Ken Chasse, 'The Admissibility of Electronic Business Records' (2011) 8(2) *Canadian Journal of Law and Technology* 105.

burdens and standards with respect to the presentation of electronic evidence. That is an entirely helpful and appropriate function for evidence law. Regarding the substance of what is to be achieved, the provision can be attacked as trite and, thereby, otiose. For as long as trials are conducted according to principles of rational verdicts, it is trite to suggest a party leading evidence needs to establish the evidence is what the party claims.[118] A party seeking to establish their case knows this is necessary as a matter of the plausibility of their case, and it is otiose to tell them so. Such criticisms may be returned to the other as, in one sense, most if not all the rules of evidence may be argued as trite to the protagonist seeking to persuade a rational deliberative process by the presentation of probative evidence. The important point for present purposes is that, as we have discussed, particularly apropos acceptance, the person seeking to introduce the electronic record, as well as those to whom it is presented, may have no reason to think it is other than that which it purports to be, notwithstanding it is not at all what it purports. The law is trite and thereby unhelpful if it merely asserts the requirement of provenance in the age of trials adjudged by IoT-derived evidence.

Similar issues arise whether the presumptions do not apply or have been rebutted. The ordinary means of authentication of machine-generated evidence is by proving that the machine was functioning correctly at the time that the evidence was generated, which may be achieved by way of lay testimony by somebody operating the relevant machine or by an expert who is able to examine its historical performance. This may involve the use of metadata or an operation log, or evidence from a specialist in 'computer forensics', which is an emerging discipline relating to the identification, preservation, analysis and presentation of ESI.[119] Indeed, a forensic data-handling expert may also be involved in the storage, extraction and 'translation' of ESI in order to copy, process and present the ESI. In such a circumstance, they may be required to provide evidence about how they handled the evidence and preserved its evidentiary integrity.[120] However, this inquiry fails to account for how the data was created and collected, what data was and was not recorded that could have been, the provenance of the data from the time it was recorded to the time it was extracted or collected for the purpose of the proceeding, and the security of the data during transmission and storage. The proper function of the device that generated evidence is merely one aspect of the identity and authenticity inquiry that must be undertaken to justify the admission of the evidence, or at least, to justify a substantial weighting being accorded to the evidence. It does not address the quality and completeness of the ESI, the storage and security of the ESI, or the constancy or integrity of the ESI itself. As such, these provisions may be critiqued as inadequate or incomplete to deal with authenticity of computer-generated evidence.[121]

Stephen Mason suggests that the authenticity of electronic evidence ought to be assessed according to five criteria. First, whether the data itself has changed since it was created, and if so, whether there is an accurate and reliable method of recording the changes. Secondly, whether the data can be demonstrated to have been continuously secure and unaltered between the time it was obtained for legal proceedings and its submission into evidence. Thirdly, whether techniques used to obtain and process the data can be tested. Fourthly, whether the data is proven to have

118 Whether a question of law or fact, evidence must be authenticated at some point (if not multiple points) in the trial, cf, above re Bryson and Perram JJ positions.

119 Stanfield (n 83) 124.

120 Ibid 125-126.

121 See ibid 191.

been generated by the purported device. Fifthly, whether technical evidence of the data's integrity as being trustworthy and reliable has been furnished.[122] This approach is reminiscent of the repealed s 59B in South Australian evidence law. The starting criterion remains problematic for the reasons we have discussed. How is 'whether the data itself has changed since it was created' to be questioned and evidenced? In cases of fraud or like actions, retrieval of data or computer images may evidence the alteration or destruction of electronic records from that which purportedly appear on current searches of the stored data.[123] Those cases rely on the manipulation being deliberate and the product of human input. The growth of autonomous methods of amassing electronic evidence present a significant hindrance to the content or presentation of 'change' in the electronic record. The issue of authentication is not necessarily that there has been alteration but that the original record is erroneous. A matter which the absence of human oversight makes difficult to detect or even pinpoint to an origin for analysis.

We acknowledge our criticisms of existing and proposed authentication provisions and methods, without providing a framework for their replacement. Our purpose is to identify the lacunae in the existing law with respect to authentication that, principally, results from a human-centric paradigm for the authentication and rationalisation of evidence. That paradigm must shift as evidence is increasingly presented from autonomous technological functions. Regarding how authentication might be better achieved in third and future wave autonomous technology is, we suggest, a question for computational science and its associated engineering disciplines. With respect to the shift needed in the law, the question to be confronted is whether there is need and merit to distinguish between evidence generated by computational processes based on the ordinary level and requirement of human input. This bedrock question may inform safeguards the law puts in place with respect to accepting the provenance and use of certain types of electronic evidence.

V CONCLUSION

The unique character of IoT-derived ESI, relative to traditional documentary evidence, and the volume that is and will continue to be (increasingly) generated, necessitate careful consideration of whether pre-trial litigation procedures and intra-trial evidentiary rules sufficiently deal with the unique character of this ESI. First, issues relating to the obtaining of ESI arise, including how and from where or whom the relevant data may be obtained. This turns on whether the possessor of the data is a party to the litigation, and how and where the data is stored. Much of the data generated by eObjects is stored on the cloud and is discoverable by anyone with access to that data through the relevant eObject or through other means. Once the identity, availability, and possession of the ESI are determined, the question turns to whether discovery (or production by different means, such as by way of subpoena or notice to produce) is justified, and how it may be put into effect so as to minimise the cost and delay of litigation. This may require the court, the legal representatives and the parties to carefully consider the necessity and utility of the discovery of IoT-derived information, and how discovery orders can be crafted in either a restrictive or prescriptive way. The volume of data may necessitate a creative or technology-assisted

---

122 Stephen Mason (ed), *Electronic Evidence* (LexisNexis Butterworths, 3rd, 2012) [5.01]-[5.37].

123 This case strategy is often underpinned by seeking pre-action orders, such as Anton Piller or search orders.

solution, to ensure proportionality between the possible utility of the process and its cost.

We argued that IoT-derived evidence is not subject to the hearsay rule. The inapplicability of this evidential safeguard is magnified by the difficulties inherent in the authentication of IoT-derived electronic evidence. Despite being the output of largely or wholly autonomous technology operating absent human input or intervention, this IoT-derived ESI requires or relies on humans to authenticate it. The more divorced the data generation is from human input, the greater the need to verify its identity, integrity, provenance and authenticity. Putting pragmatic difficulties aside, the very nature of IoT-derived electronic evidence, and the eObjects that generate it, necessitates especial attention to addressing integrity and authenticity, as (i) electronic evidence is liable to be unalterably and untraceably manipulated, intercepted or or modified; (ii) electronic evidence from eObjects may be altered by inadvertent or accidental actions; and (iii) electronic evidence may mislead or misrepresent on account of ineffectual or intermittent use by humans. The UEL does not provide mechanisms that are apposite to these foibles of IoT-derived ESI.

We have discussed why certain legislative presumptions concerning relevance and authenticity prescribed by the UEL fall short of addressing crucial concerns around the security of the eObject that generated the relevant data, the security of the data during transmission and storage, and the authenticity of the ESI itself, as opposed to the reliability and authenticity of the process or device that generated it. The absence of a robust and prescriptive process or legislative test for the authentication of such evidence raises concerns about whether IoT-derived electronic evidence falls into an evidentiary fissure that lacks sufficient prophylactic measures to properly regulate its admission and assessment. A doctrinal safeguard ought to be the subject of further discourse and, perhaps, reform.

***