A Guide to Autonomous Machine Testimony

2020-2021

A Guide to Autonomous Machine Testimony

Smart objects have taken over our homes, workplaces and communities, and over the coming decades, the volume of legally admissible data from these devices is likely to be more. The new culture is to have voice-activated technology as digital assistants, smart appliances, and personal wearable devices.

Lawyers may have to represent clients in cases dealing with evidence, witnesses, or contracts, all relying on immutable digital proof such as time-stamped video and audio recordings. The lawyers may need to specialize in addressing the data issues concerning the domains such as digital twins and personas, surveillance capitalism and digital privacy rights. A pivotal step is getting this information admitted as evidence. Firms need to start building expertise around the admissibility and verifiability of data collected by smart technology-enabled devices.

The Smart Home is the Nest of the Internet of Things

Network and internet-connected devices, also referred to as the Internet of Things (IoT) are creating a nervous system within what has been traditionally recognized to be the most private of spaces: the home. Fundamentally, the IoT is a system to gather and assimilate immense quantities of information that amount to private surveillance of the user's activities, preferences, and habits in his own home. This information is to optimize the function of the given object.

The first Internet of Things privacy study, a joint academic collaboration between Northeastern University and Imperial College London, examined the data-sharing activities of 81 different "smart" devices that are omnipresent today in people's homes. These included immensely popular consumer products produced by tech giants, including smart TVs, smart audio speakers and video doorbells. The teams of researchers (one in the US and one in the UK) conducted 34,586 experiments to quantify exactly much data these devices were collecting, storing and sharing.

The researchers' findings were staggering, 72 of the 81 IoT devices shared data with third-parties completely independent of the original manufacturer. Furthermore, the data that these devices transmitted went far beyond rudimentary information about the physical device being used. It included the IP addresses, specifications of the device and configurations, usage habits, and location.

Today's economy is a surveillance economy – one that is dead set on acquiring "behavioral surplus", or the digital data generated as a by-product of human interaction with a wide variety of devices. These include, but are not limited to cell-phones, self-tracking devices, social media interfaces, and smart home devices anticipated to be a USD 27 billion market by 2021. As the number of devices generating digital records of usage grows exponentially, and as their records of usage tracks, not just communications but also movement, domestic habits, and even sleep patterns, this behavioral surplus can yield an elaborate account of human behavior.

The most familiar example may be that of the location-tracking component of cell phones. Cell phones transmit a rich, comprehensive account of individuals' movements in time and space which can be monetized. So tenacious is this feature that even when location-tracking apps are switched off, and SIM cards are removed from the device, some phones continue to collect location material by enabling triangulation via local cell towers, and generating distinctive "mobility signatures".

continued on next page ▸

"The first rule of any technology used in a business is that automation applied to an efficient operation will magnify the efficiency. The second is that automation applied to an inefficient operation will magnify the inefficiency."

– Bill Gates

Inside the home, digital assistants such as Siri and Alexa are capable of recording and transmitting ambient conversations; more insidiously, the development of lidar sensors, which would map both movement and behavior, is reported to be underway. 'My Friend Cayla' is an interactive toy that captures conversations between the doll and its children users, and then proceeds to transmit those conversations to the manufacturer for further uses.

The Privacy Issues inherent to these Smart Devices

Other studies support the notion that any device connected to the Internet can be used as ad tracking devices. What really raises IoT privacy issues is how that device-divulged information and data is being employed. If it were used for personalization and customization, then that would have been understandable to a degree. For instance, information about which devices are being used to watch Netflix's streaming content might help them to optimize the quality of their streams.

However, IoT privacy experts have suggested that actual personal data "leaking" from home is being harnessed to construct sophisticated profiles of users, based on their usage habits. It is even more troubling, from a privacy perspective, that some of this data involves personally identifiable information such as exact geolocation data, social media data, and unique device information. All of this data can easily coalesce in order to deduce the identity of the user; this very data falls into a goldmine for advertisers, who strive to learn as much as they can about users so that they can optimize the relevance of the ads they issue.

The 'Testimony' these devices issue

In March 2018, Facebook disclosed that the political consultancy, Cambridge Analytica had accessed the personal data through improper means of up to 87 million Facebook users. What was worse, Facebook failed to notify its users of the colossal breach until long after it learned about it. It received a whopping USD 5 billion sanctions from the Federal Trade Commission for its privacy failures, along with a USD 100 million fine from the US Securities Exchange Commission.

Despite this, their privacy practices remain amorphous. To illustrate the same, some terms in the Supplemental Portal Data Policy of the 2019-released Portal smart display can be studied.

The Data Policy states that when portal's camera and microphone are on, Facebook collects camera and audio information, although it states that it does not listen to, view the contents or keep any video or audio calls on the portal.

The Data Policy further elucidates upon how this information is shared, stating that they may also share voice interactions with third-parties where we have a good faith belief that the law requires us to do so. It also states that, when independent apps, services, or integrations are used on Portal, Facebook shares information with them about the Portal device, the device name, IP address, zip code, and other information to help them provide the requested services.

The terms of service agreements like the aforementioned one are blatantly ambiguous and bear great privacy flaws. However, a lot of consumers have rationalized that the trade-offs are worth it; while privacy may be a concern, at the end of the day, convenience reigns supreme. The promise of enhanced conveniences, as well as the reduction in household costs, is a big overriding factor that explains why consumers continue to purchase and use these devices despite privacy risks.

continued on next page ▸

*"Automation does not need to be our enemy.
I think machines can make life easier for men,
if men do not let the machines dominate them."*

– John F. Kennedy

Having said that, when a security breach happens, the impacts are borne by device owners and wider society, and more often than not, the makers of these devices are indemnified. The regulatory oversight that privacy breaches invite and the privacy infrastructure of different jurisdictions will be explored below.

Digital Privacy in the US

In 2017, 143 million American consumers' personal information was exposed in a data breach at Equifax; in 2013, 3 billion Yahoo accounts were affected by an attack; in 2016, Deep Root Analytics accidentally leaked personal details of nearly 200 million American voters; in 2016, hackers stole the personal data of about 57 million customers and drivers from Uber Technologies Inc. Despite these record-shattering data breaches and inadequate data-protection practices, only piecemeal legislative responses have been produced at the federal level. While most Western countries have already adopted comprehensive legal protections for personal data, the United States, home to some of the most advanced tech and data companies in the world is possessive of only a patchwork of sector-specific laws and regulations that utterly fail to adequately protect data.

The American Fourth Amendment

The Fourth Amendment of the US Constitution declares inviolate "the right of the people to be secure in their persons, houses, papers and effects." It protects against unreasonable government intrusions by establishing a certain right to privacy enforceable by the individual as against the world.

The essence of the Fourth Amendment is clearly to restrain unwarranted government action against the individual: it is the expression of the framers' intent to secure the American people from intrusion by the state, in the form of unreasonable search and seizure. However, the Court does not properly recognize how the Fourth Amendment protects digital privacy; virtual access by law enforcement threatens the security of citizens in their houses.

Data Breach Notification Law of 2003

California enacted the first data-breach notification law in 2003, and forty-eight states followed suit. They passed laws that require individuals to be notified if their information is compromised. However, the shortfall here is that these laws have different and sometimes incompatible provisions regarding what categories and types of personal information warrant protection, which entities are covered, and what constitutes a breach.

The US legal framework on personal data has not meaningfully changed in several decades; on the other hand, the European Union has enacted multiple data-protection directives. What with the General Data Protection Regulation, the European Union has become the focal point of the global dialogue on individual data privacy. In contrast to the US, the laws in the EU protect all personal data, irrespective of who collects it or how it is processed. Countries such as Canada, Israel, and Japan, have all pivoted towards creating privacy regimes which are compatible with the EU's GDPR contrary to the patchwork approach of the United States. This puts US companies at a disadvantage globally as emerging economies adopt simpler, and often more EU-style, comprehensive approaches.

continued on next page ▸

"I know a lot about artificial intelligence, but not as much as it knows about me."
- Dave Waters

Digital Privacy in the EU

GDPR – General Data Protection Regulation

On 25 May 2018, the European Union enacted the world's toughest rules in order to protect people's online data - the General Data Protection Regulation (GDPR). At a time when most technologically engaged people are entrusting their personal data with cloud services, and breaches are a daily occurrence, Europe signaled its firm stance on data privacy by employing a versatile tool, the GDPR and The GDPR, which permits people to request their online data and restricts how businesses obtain and handle that very information, has cemented Europe in its role as the world's foremost tech watchdog. With penalties reaching into the tens of millions of euros, the GDPR's efficacity is cemented by its promise to levy harsh fines against violators of its privacy and security standards.

The GDPR consists of privacy measures that let people assume autonomy over the trail of information they leave behind whilst engaging in a plethora of online activities, whether it be browsing social media, reading the news, or shopping online. Not only does it allow for individuals to request the data, but also demand that it be deleted. The GDPR also mandates that businesses have an obligation to clearly detail how someone's data is being handled, whilst clearing a higher bar to target advertising using personal information. Companies face fines if they do not comply, with tech giants risking penalties greater than USD 1 billion. Privacy groups preparing class action-style complaints under the new law have the opportunity to put even more legal pressure on companies.

G.D.P.R. - Personal Data

Pursuant to Article 5 of the GDPR, the Principles relating to the processing of personal data delineate that personal data shall be processed lawfully, fairly, and in a transparent manner. They state that it may be collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes. Furthermore, it states that personal data shall be adequate, relevant and limited to what is necessary for relation to the purposes for which they are processed ('data minimization').

GDPR – Compensation and Liabilities

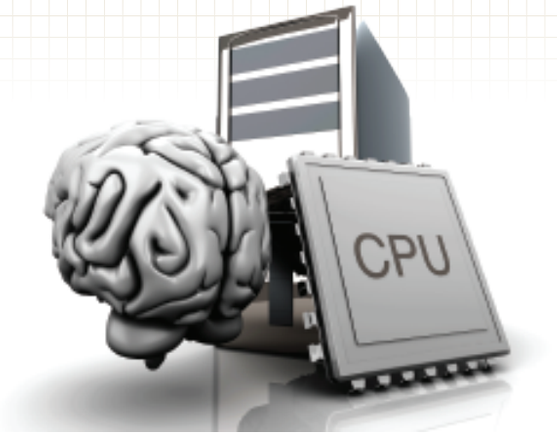
Article 82 of the GDPR categorically states that any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.
Furthermore, the entity that shall be liable for the damage caused by processing that infringes upon this Regulation will be the controller, i.e. the agency that determines the purposes and means of processing the data.

By means of the GDPR, the EU has been striving to position itself as the responsible alternative to surveillance capitalism and authoritarian state control. To further that end, in late February, the European Commission released its long-awaited white paper on artificial intelligence (AI). The paper was seen as the world's first pan-national attempt to regulate AI and forms part of the European Union's grand plan for regulating.

continued on next page ▸

"The potential benefits of Artificial Intelligence are huge, so are the dangers."

- Dave Waters



Despite this, many AI applications with far-reaching societal consequences still fall outside the scope of the regulatory proposal. For example, data brokers that use AI to predict people's identities and interests, or the many ways in which AI is used to target advertising today, furthering and entrenching corporate surveillance, remain unaddressed.

Digital Privacy in India

Personal Data Protection Bill

Catalyzed by Europe's General Data Protection Regulation, the Indian Parliament published the Personal Data Protection Bill on 11 December 2019; it was introduced by Ravi Shankar Prasad. As of 17 December 2019, the Bill is being analyzed by a Joint Parliamentary Committee (JPC) in consultation with various groups.

The legislation builds on the GDPR that gave residents there the ability to request and better control their online data; in a fashion that mirrors the GDPR, India's Bill would force global internet companies to seek explicit permission for most uses of an individual's personal data, and facilitate people's demand that the same be erased.

Notably, however, the proposal would place fewer restrictions on the government's own use of sensitive data on its residents, which include fingerprint and iris scans as part of the Aadhaar national ID system, and its detailed surveys of who would receive the government benefits in every household. On paper, the data protection rules are applicable to government agencies. However, the law would grant the central government with broad powers to exempt any public entity from the requirements for securing national security or public order. This is reasonably concerning given that, in India, the government is the largest collector of data.

Alongside the Bill, India also proposed the manifestation of a new entity, the Data Protection Authority which would be charged with writing specific rules, the monitoring of how corporations are applying them, and the settlement of disputes. That agency would surely wield a great deal of power to decide whether a data breach must be disclosed to the people affected and setting policies on whether search engines should be exempt from the consent requirements. So, the question that follows is whether this new data authority would have the required bandwidth to manage all of these mammoth responsibilities, given that there is very minimal legal precedent to guide it.

Right to Privacy

This pending Bill could be regarded as the technological offshoot of the upholding and endorsement of the Right to Privacy as a fundamental right by the Supreme Court on 24 August 2017. This verdict was an immense setback for the government which insists that privacy is not an inalienable fundamental right guaranteed under the constitution since the days of yore.

When the Aadhaar database was launched in 2009, the authorities had gift wrapped it as a voluntary scheme to weed out corruption, whilst passing on welfare benefits to the neediest citizens. However, in the years following that, it had been made mandatory for filing tax returns, opening bank accounts, securing loans, buying and selling property or even making purchases of 50,000 rupees (USD 780; GBP 610) and above.

continued on next page ▸

"Predicting the future isn't magic, its artificial intelligence."

- Dave Waters

This was likely to have helped the authorities create a comprehensive profile of a person's spending habits; the handing over of such data to a government which did not believe in people's right to privacy was a worrisome prospect. Therefore, the judges' 2017 ruling that the right to privacy was "an intrinsic part of Article 21 that protects life and liberty" was historical one; it assured citizens that they are the masters of their bodies, minds, and lives.

Digital Privacy in the UAE

While the UAE does not have a comprehensive data protection law at its federal level, there are a number of laws in place governing privacy and data security in the UAE. There are exist sector-specific data protection provisions in certain laws.

Article 379 of the UAE Penal Code

The most relevant is Article 379 of the *UAE Penal Code*. This law strictly prohibits a person "who, by reason of their profession, craft, situation or art, is entrusted with a "secret," from using or disclosing that "secret," without the consent of the person to whom the secret pertains, or otherwise in accordance with the law." A breach of Article 379 is punishable with imprisonment of a minimum of one year or a fine of a minimum of AED 20,000, or both.

An inadequacy here is that the term "secret" is undefined; however, it can broadly cover the concepts of personal data, as defined in several other data protection laws (for instance, name, date of birth, gender and religion). The terms "use" or "disclose" also remain undefined; however, the terms can again broadly cover the concepts of "processing" and "transfer" respectively. The transfer can be to a third-party or to another entity within the UAE or overseas.

Article 379 permits the use or disclosure with the consent of the person to whom the secret pertains. Therefore, in order to mitigate the risk of a breach of Article 379, it is generally suggested to obtain the consent prior to the use or disclosure of personal data. This can be obtained by a signature on a paper consent form or a tick on an electronic consent form would both be perfectly acceptable.

Notably, in December 2015, the Dubai Government published the *Dubai Law Number 26 of 2015 on the Regulation of Data Dissemination and Exchange in the Emirate of Dubai, the Dubai Data Law*. The *Dubai Data Law* was constructed in order to collate and manage data concerning Dubai and, if appropriate, to publish it as open data or ensure that it is shared between authorized persons. This *Law* is unique for it provides a government with the power to require the designated entities of the private sector to provide it with information held by the company concerning a city, for making that information Open Data.

Conclusion

Jurisprudence is at a junction where relatively new, but pernicious technologies demand a course-correction. The business model of smart devices amounts to private surveillance, and society has accepted this to the extent that it improves services through interconnectivity and customization. However, what is evident is that these devices have a range of intelligence, and each smart object represents a vector for remote access by black hat hackers and government agents alike. Without an affirmative recognition by the courts that the data-rich smart home is secured by legislation, privacy rights are universally vulnerable to digital abuse.

STA Law Firm's offices across GCC

Abu Dhabi Office

Advocates and Legal Consultants
23 A, Level 23 Tamouh Towers
Marina Square, Reem Island
Abu Dhabi, United Arab Emirates

Tel: +971 2 644 4330
Fax +971 2 644 4919

ADGM Office

3517, Al Maqam Tower
Abu Dhabi Global Markets Square
Abu Dhabi
United Arab Emirates

Tel: +971 2 644 4330
Fax +971 2 644 4919

Dubai Office

Advocates and Legal Consultants
Office 1904, Level 19, Boulevard Plaza,
Opposite Burj Khalifa
Dubai, United Arab Emirates

Tel: +971 4 368 9727
Fax +971 4 368 5194

Sharjah Office

48-1F, Next to Abu Dhabi Islamic Bank
Near Hamriyah Free Zone Headquarters,
Hamriyah
Sharjah, United Arab Emirates

Tel: +971 6 513 4270
Fax: +971 6 526 4027

Bahrain

Advocates and Legal Consultants
Level 22, West Tower
Bahrain Financial Harbour
King Faisal Highway
Manama
Kingdom of Bahrain

Tel: +973 1750 3045

Qatar

Level 22, Tornado Tower
West Bay, Doha
Qatar
PO Box – 27774

Tel: +974 44294827

RAK Office

Office 501-A, Level 5, Building 4
Ras Al Khaimah Free Trade Zone
Ras Al Khaimah,
United Arab Emirates

Tel: +971 7 204 2180

Fax: +971 7 204 2181

Fujairah Office

Creative Tower
Creative City - Media free zone
Fujairah,
United Arab Emirates

Tel: +971 7 204 2180

Fax: +971 7 204 2181

For a free subscription request, you can e-mail us at:
corporate@stalawfirm.com
with your name and address.
www.stalawfirm.com

ISBN 978 - 9948 - 22 - 445 - 7

Office 1904, Level 19,
Boulevard Plaza, Tower 1,
Opp. Burj Khalifa, Dubai
United Arab Emirates

Tel: +971 4 368 9727

corporate@stalawfirm.com
www.stalawfirm.com