the global voice of the legal profession

Report of IBA Legal Practice Division Working Group

Digital identity: principles on collection and use of information

Table of Contents

Report of IBA Legal Practice Division Working Group

Digital identity: principles on collection and use of information

Working Group members

Sylvia Khatcherian *Working Group Chair*

Erik Valgaeren *Working Group Deputy Chair; IBA Technology Law Committee*

Peter Bartlett *IBA LPD Council Member; IBA Media Law Committee*

Laura Christa *IBA LPD Council Member; IBA North American Regional Forum*

Anurag Bana *IBA Legal Policy & Research Unit*

Background and focus

The pervasive use of new modes of communication and transaction of business, for personal and professional purposes, is creating information relating to users that goes beyond 'who am I'. It is no longer about personally identifiable information as recognised in various existing legal frameworks, but about a broader set of digital information, including behavioural information that is provided or caused by or related to a particular individual, such as where am I, what am I doing, who am I with, what do I read, what do I buy and the like (hereinafter digital identity).

The EU Council Future Group predicted a digital tsunami of personal data. The Council Presidency stated that [every] object the individual uses, every transaction they make and almost everywhere they go will create a digital record.[1] As more and more individuals, in both their private and professional lives, use or rely on information they provide or which is implicated by other users, opting out of using these new modes of communication is no longer a realistic option. This is a global phenomenon.

The extent of collection and use of this type of information however is not always known by the user, nor is it readily ascertainable. Today, the user is not fully in control of his or her digital identity. Unless one knows when such information is being collected, the extent and who it is shared with, the individual is not in a position to control how his or her digital identity is used and how it is protected.

Moreover, there are many other players who claim or expect various types of rights in such information, eg, the platform or service providers, mobile applications providers, third parties interacting with the users, data brokers. Some of these players rely on their terms of use and privacy

1 Republic of Portugal Public Security, Privacy and Technology in Europe: Moving Forward, European Union Council Presidency Paper 2007 <http://www.statewatch.org/news/2008/jul/eu-futures-dec-sec-privacy-2007.pdf>

policies, which attempt to contractually set out, by the users click of agree, the types of rights in such information as between them and the user. These terms of use and privacy policies however are often complex and unclear, use very broad language, and where they do offer privacy setting options or certain opt outs, are often difficult to figure out and not very meaningful.[2] Consequently, the claimed rights of control over, and use of, digital information may not correlate with the users expectations of privacy.

The impact of use of an individual's digital identity without their knowledge and expectation can be significant and is often a negative and unwelcome surprise.[3] In a recent example, a subset of Facebook users found themselves unknowing participants in an experiment by Facebooks data scientists who manipulated news feeds to see if the content of the feeds, negative or positive, impacted the emotion of the users as displayed through the users' posts. Facebooks terms of use allow Facebook to use the users' data for analysis, testing [and] research. Should users have expected that this type of research, which went beyond product testing, was within the terms of use they clicked through?

The existing legal definitions of identity and the attendant protections, typically around personally identifiable information (PII), are not adequate to cover the full scope of digital identity. Legal rights in information are contextual, eg, PII, or trade secrets, and under civil law, information as such is not a legal category. Regulators and legislative bodies in various jurisdictions have begun to consider measures to fill in the gaps, typically within the framework of existing data protection laws in their respective jurisdictions.[4] These efforts are of course jurisdictionally bound, and they may or may not result in a harmonised approach to addressing collection and use of digital information. The Working Group considers it important that a global approach be adopted to this issue as it is a global issue for the global economy.

---

2 Summary of the review done by the IBA Legal Policy Research Unit in August of 2013 entitled Social Media Platform Providers – A Short Study. See Annexure. In its 2015 'Updated Terms and Policies' Facebook has sought to 'better explain how [they] get and use information, to help users 'Understand How Facebook Works and How to Control Your Information'. A report commissioned for Belgiums privacy commissioner has concluded that Facebooks updated policies and terms of use give users a false sense of control over their data, and is in violation of European privacy law. See report, <http://www.law.kuleuven.be/icri/en/news/item/facebooks-revised-policies-and-terms-v1-1.pdf>

3 Samuel Gibbs, Europes next privacy war is with websites silently tracking users (The Guardian, 28 November 2014) <http://www.theguardian.com/technology/2014/nov/28/europe-privacy-war-websites-silently-tracking-users> ;
Christopher Hope, Facebook can access your mobile, take pictures and video – warning (The Independent, 28 November 2014) <http://www.independent.ie/business/technology/facebook-can-access-your-mobile-take-pictures-and-video-warning-30782260.html>; Special report Getting to know you (The Economist, 13 September 2014) <http://www.economist.com/news/special-report/21615871-everything-people-do-online-avidly-followed-advertisers-and-third-party>

4 FTC staff report recommends ways to improve mobile privacy disclosures (United States of America Federal Trade Commission press release, 01 February 2013) <http://www.ftc.gov/news-events/press-releases/2013/02/ftc-staff-report-recommends-ways-improve-mobile-privacy>;
European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>;
European Commission, Proposal for a Directive of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data by competent authorities for the purposes of prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and the free movement of such data COM(2012) 10 final <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_10_en.pdf>;
OECD (2011), National Strategies and Policies for Digital Identity Management in OECD Countries, OECD Digital Economy Papers, No. 177, OECD Publishing <http://dx.doi.org/10.1787/5kgdzvn5rfs2-en >;
OECD (2007), At a crossroads: 'Personhood' and digital identity in the information society, STI Working Paper 2007/7 <http://tinyurl.com/p8hh34s>;
(ACMA) 2013 Australian Government, Privacy and personal data: Emerging issues in media and communications, Occasional Paper 4 <http://www.acma.gov.au/~/media/Regulatory%20Frameworks%20and%20International%20Coordination/Information/pdf/Privacy%20and%20digital%20data%20protection%20Occasional%20paper%204.pdf>;
Greenleaf, Graham and Tian, George, China Expands Data Protection through 2013 Guidelines: A Third Line for Personal Information Protection (With a Translation of the Guidelines) (April 16, 2013). Privacy Laws & Business International Report, Issue 122, 1, 4-6, April 2013; UNSW Law Research Paper No. 2013-37; UTS: Law Research Paper No. 2014/15 SSRN. <http://ssrn.com/abstract=2280037>

Working Group objectives

With this backdrop, the Working Group undertook to develop a set of high-level Principles around the collection, use and sharing of digital identity information that could serve as the basis for engaging in dialogue with all relevant stakeholders, including representatives of platform and service providers, mobile application and location services providers, intermediaries such as data brokers, as well as governmental agencies and other interested organisations. The intention was not to seek to control the providers nor to slow the development of the sector. The train has already left the station in terms of the way that the industry is using, and could in future use, technology to process information. As with the White House's report, 'Consumer Data Privacy in a Networked World'[5], the intention is to provide sensible balanced rules of the road for the 'information society'.[6]

At the outset of this effort, the Working Group considered whether the scope of its work should include circumstances under which such information can be provided to governments, but decided to initially limit its focus.[7]

The proposed Principles developed by the Working Group are outlined in the attachment to this report. These Principles are intended to provide a foundation that withstands rapid technological developments and reflect users' expectations as they evolve. The overarching aim is to provide for **transparency, responsibility** and **security,** with the underlying premise that users should have control over their identifiable information. The ultimate objective is to arrive at a set of Principles that would be agreed to and adopted by all stakeholders, following consultation and input.

Considerations underpinning the Principles

Rights over data

At present, data aggregators behave as if they are the owners of the personal information they are mining and processing. The Working Group believes this to be an error: it would ultimately lead to the conclusion that a search engine could 'own' an individual's identity online. The Working Group believes it is more appropriate to ascribe ownership of personal information to the persons to whom that information relates. However, this goes hand in hand with a recognition that the notion of ownership of this new form of informational property will have to be developed as the digital economy develops, and is likely to be more nuanced than our notion of ownership of land and chattels in what might be called the 'old economy'.

A possible useful way of analysing the issue is to make an analogy with the Roman law distinction between rights 'in rem' and rights 'in personam'. It would be appropriate to reward the skill, labour and investment of the person assembling databases of information. Nevertheless, the in personam right to exploit the information would be subject to an individual's wish to assert their in rem right

5 The United States of America White House Report Consumer Data Privacy in a Networked World (February 2012) <http://www.whitehouse.gov/sites/default/files/privacy-final.pdf>

6 OECD (2007), At a crossroads: 'Personhood' and digital identity in the information society, STI Working Paper 2007/7 <http://tinyurl.com/p8hh34s>

7 A set of principles on the circumstances under which information can be provided to governments have already been developed by the Global Network Initiative (GNI), a multi-stakeholder group of companies, civil society organisations (including human rights and press freedom groups), investors and academics, who have created a collaborative approach to protect and advance freedom of expression and privacy in the Information and Communications Technology sector. <https://www.globalnetworkinitiative.org>

to have their information removed or de-personalised from the database and to receive appropriate payment or other compensation for the use of their property.

This would create a legitimate right to use the information on the part of data aggregators, and provide clarity for service providers and third parties. This principle would require greater transparency from information holders as to the nature and detail of information held about individuals. This would also require collectors, such as providers of social networking sites and mobile apps, to improve the effectiveness and clarity of their privacy policies and provide meaningful choices and incentives to users on the use of information they provide.

The United States Freedom of Information Act (FOIA) gives an individual the right to ask any public sector organisation for all the recorded information they have on any subject. Mini FOIAs or Data Subject Information Access Rights, similar to rights under the European Data Protection Directive, could be adapted to facilitate individual requests for recorded identifiable information about the user where the information is used by the collector to make decisions that will affect the identifiable user, eg, approve or deny services.

While there was general agreement that there is a need for a right for individuals to have their personally identifiable information removed in certain circumstances, analogous to the 'right to erasure' under the European Union's General Data Protection Regulation Article 17, the circumstances under which such a 'right' should be available are still under consideration. The recent divergent court decisions addressing right to erasure under the data protection laws (discussed in the Principles attached) are informative on the considerations implicated, but, in the view of the Working Group, more work needs to be done to formulate the parameters for a balanced and workable approach.

Data is sold to third parties, and it is in this way that the commercial value is realised. Can consumers be given control over the monetary value of this data (as advocated by Tony Fish in mydigitalfootprint.com)? If this is not possible, would users in personam rights to remove or de-personalise data extend to enforcement against third parties? The proposed California Right to Know Act (since put on hold and facing opposition from industry as being unworkable) would have allowed California residents to demand copies of all information retained and the categories that were disclosed to third parties over the past 12 months, as well as contact information for the third parties.

Protection of data

As information grows in value as an asset class, the fiduciary duty of those who deal with the assets for profit or otherwise will rise. There is a need to secure as far as possible the reliability and authenticity of information in the digital world. The possibility of fraud can never be eliminated, but the law should be leading the digital world to an acceptance of the neighbour principle in relation to use of information. There should be consequences for loss caused by the reckless or careless use of information by those who are 'holding' the information or for the reckless or careless creation of misinformation about an individual.

Third parties are now relying heavily on digital data as a mine of information. Does the duty lie with

the service provider to authenticate the data that is posted, or the third party who is relying on the information?

It may be that there is tension between increasing security barriers and improving the process to validate identity, and ease of communication and increasing online activity.

There may also be a need to protect the information by preventing its destruction. If users view a service provider as a safe keeper, eg, by the nature of the service being provided, and the provider undertakes to act as a 'host' and the information is destroyed, then users rights to the information may be violated.

Enforcement mechanism

In addition to setting out the Principles, there is a need to create enforcement mechanisms that are:

- Quick;
- Effective;
- Consumer friendly;
- Low cost; and
- Global in application.

The Internet Corporation for Assigned Names and Numbers (ICANN) model might be one that could be adapted for enforcing the obligation on social media and other sites to comply with requests for, eg, erasure, de-personalisation or authentication of material. The model would need to address differences in jurisdiction, and could provide for alternative dispute resolution in appropriate cases.

Either by way of transition towards or in conjunction with an enforcement mechanism "ICANN style", effective enforcement would at least require that each jurisdiction has a clearly identified body which would act as a focal point. Such national enforcement body ("NEB") should function under the auspices of a democratically elected forum or institution and operate under transparent and published rules aiming at due process, fairness and evidence based decision making. NEB's should ensure an easy access for all and a quick and cost efficient resolution of the matters being handled.

NEB's should be empowered to investigate matters both on its own initiative and further to a complaint. Staff members involved in dealing with these issues should be fully familiar with the various social media and new technologies and in house technical experts should be available to make independent assessments.

Moreover, NEB's should have at their disposal a broad spectrum of possible sanctions allowing them to respond in a way proportionate to the cases presented and the findings arrived at. While the members of the NEB should be bound by professional secrecy rules, sanctions should also include "naming and shaming" measures, including via publications of findings and decisions.

The budget of the NEB should be exclusively funded by public means and the management level of the NEB (board, counsel…) should be fully accountable for the use of the budget. Moreover, the decisions of the NEB should be subject to review by the judiciary.

NEB's would also be expected to issue opinions, recommendations and reports with a view to providing practical guidance on new developments, either in law or in the area of technology.

In addition to enforcement being effectively organized at a national level, there is a need for a formal structure for regional and even global interaction between NEB's. Such structure should allow for coordination between NEB's on cross-border matter, facilitate the exchange of information of information and expertise and contribute to the creation and propagation of best practices.

Effective remedies

In addition to an enforcement process, each jurisdiction should have a set of effective legal remedies. These should be actionable either before the NEB or before the courts, in each case on the basis of a swift and quick process.

Effective remedies should include both i) the possibility of an immediate action or intervention to end a factual threat or hazard (eg. take down or omission) under appropriate mechanisms of coercion (injunctive relief, penalties…), and ii) the proper repair of harm done, either in pecuniam or in kind. In all circumstances, an appeal level should be available where the case can be reviewed in its entirety.

Principles on the collection, use and sharing of digital identity information

Definition of digital identity

'Digital identity' information is intended to cover the broad set of information encompassed in the definition of identity, ie:

1. The collective aspect of the set of characteristics by which a thing is definitively recognisable or known.
2. The set of behavioural or personal characteristics by which an individual is recognisable as a member of a group.
3. The distinct personality of an individual regarded as a persisting entity; individuality.
4. Information, such as an identification number, used to establish or prove a person's individuality.

Overarching aim: transparency; responsibility; security

These principles should be applied taking into account the legitimate interests of both the individual user in his/her privacy and autonomy, and the interests of the information collector, eg, service or application provider, in reaping the benefits of its investment in collecting and enriching the data (eg, by combining with third party data sources) to provide services or capabilities that users value.

Transparency on the part of the collector of the information – at time of collection and throughout the period that the collector is holding the information:

- Providing user notice of:
- What is being collected and the purpose for which it is being collected;
- How the information will be used, as such, or in combination with other information;
- Who it will it be shared with, and under what circumstances;
- How long the information will be retained;
    - *Comment:* Providers should be able to retain information as long as relevant for the relationship engaged in with the user, on the basis of the transparency created up front.
- Where and how it will be stored.

Transparency principle would require that 'terms of use' and 'privacy policies' be clear, use concise language and be accessible.

Responsibility on the part of the collector and the user/provider of the information:

- Collector to provide meaningful user control options with respect to what user information will be collected and how information will be used.

- *Comment:* The control options should be reasonably tailored considering what is needed by the collector to provide the basic services, the additional benefits that will be available by providers' use of certain information, etc.
- User control options, eg, privacy settings, should also be easy to elect/implement, regardless of device used.

- User to be responsible for choosing from among available privacy settings – opt ins, opt outs, etc.
- Collector to notify users about any changes to settings due to technological upgrades or expansion of use.
- Where the collector is making decisions that will affect an identifiable user, (eg, whether to permit or cancel access to a service, put a 'flag', etc) responsibility to ensure the reliability of the third party sources of the information on which such decisions are being made.[8]
- Providing user access to identifiable information held by the collector/service provider and opportunity to correct any inaccuracies.[9]
  - *Comment:* User access right to extend only to information identifiable to a particular user. Anonymised behavioural information would not implicate privacy interest of the user. Service providers' interests in reaping the benefit of their investment in deriving such information would not be outweighed. Consideration should be given to whether anonymized data can be readily reverse-engineered. Responsibility for use of 'accurate' data also implicates responsibility on the part of the user for the accuracy of information inputted, particularly where the information is reasonably expected to be relied on by other, eg, a service provider or other users. This would not preclude a user from electing to be 'anonymous', where such option is available. Users should consider the nature of the services they want to avail themselves of, information they will be providing, as well as the reliability of the information made available, eg, by a service provider, and act/decide how to proceed accordingly. When providing information or making use of information on other users, a user should respect the integrity and privacy of such other users.
  - Right to access and correct may, under certain circumstances, need to be balanced by countervailing interests, particularly where privacy of other persons would be violated. For example, rights to access and correction under APEC Privacy Framework are subject to numerous exceptions that attempt to address this balance. Including, where the burden / expense of doing so would be disproportionate to the risk to privacy, where necessary for legal, security, or confidential commercial reasons; and where the privacy of other persons would be violated.
- Offering tools to allow a user to move his digital profile to another platform.
  - Comment: Users have often spent many years constructing their digital profile on a certain platform. As they evolve to other age categories, develop their careers and private lives, they may want to shift to new or additional social media or digital exchange platforms. In such case,

8 Analogous to US Fair Credit Reporting Act requirements around individuals right to obtain copy and correct inaccurate information in credit reports.

9 As an example, US data broker Acxiom has started offering consumers the opportunity to edit certain items of information it has on the consumer. See, <https://aboutthedata.com>

having to rebuild one's digital profile may constitute a barrier to the entry to such other medium or platform. The concept is in fact similar to the number portability for mobile telephone users. The draft EU Data Protection Regulation contains such data portability right10. However, it is still unclear how operators will need to implement this right at a practical level.

- Providing the user with the right and procedures to request destruction of user's identifiable information under certain circumstances to be developed.

- *Comment:* This is an area where it is especially difficult to balance individual interests, the interests of the general public in having access to information, and commercial interests. The competing considerations involved in 'right to erasure' / 'right to be forgotten' were highlighted in the recent case before the European Court of Justice involving Google.[11]

- On the scope of the data subject's rights under the EU Data Protection Directive[12], the ECJ sided with the view that a data subject may oppose the indexing by a search engine of personal data relating to him where their dissemination is prejudicial to him and his fundamental rights to the protection of those data and to privacy, which encompass the 'right to be forgotten', override the legitimate interests of the operator of the search engine and the general interest in freedom of information. The Court ruled that those rights 'override, as a rule, not only the economic interest of the operator of the search engine but also the interest of the general public in finding that information upon a search relating to the data subject's name. However, that would not be the case if it appeared, for particular reasons, such as the role played by the data subject in public life, that the interference with fundamental rights is justified by the preponderant interest of the general public in having, on account of inclusion in the list of results, access to the information in question.'

- The decision of the ECJ on the right to be forgotten under the EU Data Protection Directive is fairly sweeping – it is 'without it being necessary in order to find such a right that the inclusion of the information in question in that list causes prejudice to the data subject'.[13]

- Meanwhile, the balancing test as proposed by the ECJ has led other EU jurisdictions to reject applications for the 'right to be forgotten'. For example, a Dutch court confirmed that the right to be forgotten is not an absolute right, and that the right to privacy has to be balanced against the rights and interests of internet intermediaries, of the editors whose publications

---

10 Article 15.24 of the draft Regulation provides that "the data subject shall have the right to obtain from the controller a copy of the provided personal data in an electronic and interoperable format which is commonly used and allows for further use by the data subject without hindrance from the controller from whom the personal data are withdrawn. Where technically feasible and available, the data shall be transferred directly from controller to controller at the request of the data subject.

11 In Case C-131/12 Google Spain SL, Google Inc. v. Agencia Espanola de Proteccion de Datos (AEPD), Mario Costeja Gonzalez, the European Court of Justice was presented with Googles appeal from AEPDs decision upholding an order directing Google to adopt measures necessary to withdraw certain personal data relating to Mr. Costeja Gonzalez from its search results and to prevent access to the data in the future. The personal data was a 1998 article in the newspaper La Vanguardia, in which Mr. Gonzalezs name appeared for a real-estate auction connected with attachment proceedings for the recovery of social security debts. Mr. Gonzalez had requested that Google be required to remove or conceal this information from the results of searches on his name, stating that the proceedings in the news article had been fully resolved for a number of years and that reference to the data was now entirely irrelevant. Mr. Gonzalez had also requested that the source, La Vanguardia, be required either to remove or alter the pages containing the data from its database. AEPD rejected Mr. Gonzalez complaint against La Vanguardia, taking the view that the initial publication of the information was legally justified.

12 Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data <http://eur-lex.europa.eu/LexUriServ/LexUriServ.do?uri=CELEX:31995L0046:en:HTML>

13 As some confusion arose on the meaning and impact of this decision, the European Commission issued a FAQ document entitled Myth-Busting – the Court of Justice of the EU and the 'Right to be Forgotten', 18 September 2014. <http://ec.europa.eu/justice/newsroom/data-protection/news/140918_en.htm>

are being referenced and of the users of the internet.[14] The court recognised that committing a crime may indeed have long term negative consequences for the perpetrator but emphasised that data subjects have to face the consequences of their actions. The long term availability on the internet of information relating to such conviction in the court's view is relevant information about the person of the perpetrator and cannot easily be considered as excessive, irrelevant or unnecessarily defamatory. The court also held that restraint should be applied when imposing limits to the functioning of search engines.

- The draft EU Data Protection Regulation embraces this new right[15] and certain non EU jurisdictions appear to embrace the concept as well.[16] In the current state of affairs, it is however not clear what this right really encompasses and against whom it can be enforced. Moreover, in most non-EU jurisdictions no such right appears to exist. For example, the Working Group does not feel that there should be an unfettered right of erasure that would allow persons to rewrite history at their leisure. At the same time, the Working Group does feel that there should be appropriate rights and remedies to avoid that persons are put in a false light in the way their digital identity is being presented or reflected on social media.

- In terms of the remedy provided, it should not be left to the service providers to undertake a balancing act between competing interests, such as the digital identity rights of the individual, the right of access to information for the public at large or the freedom of expression for the press. If the idea is that the data aggregators should accommodate a kind of notice and take down, the criteria to be applied should be straightforward so there is little room for interpretation. If more sophisticated interest balancing exercises would be required, this should be rather left to courts or to supervisory authorities with the possibility of a subsequent review by a court.

- **Security –** at each step of the life cycle of information collection, use and disposition to ensure trust of the entire system.

  - Collector should implement adequate safeguards to protect the security of the identifiable information from unauthorised access or erasure, commensurate with the level of sensitivity of the information being collected.

  - *Comment:* An element of security is proper authentication. The weaker the authentication in a system, the less the trust. Some collectors/service providers have an incentive to offer stronger authentication, but also balance the user experience and ease of access. The level of security should be commensurate with the level of sensitivity of the information being collected. Currently, with social networking platforms, providers and users seem to have made a trade-off between stronger authentication steps and user experience, ie, ease of use

14 Court of First Instance of Amsterdam, 19 September 2014 (summary injunction) <http://uitspraken.rechtspraak.nl/inziendocument?id=ECLI:NL:RBAMS:2014:6118> In that case, a person convicted of being accessory to a murder attempt applied for the removal of references to publications that implicating him and his conviction.

15 European Commission, Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) COM (2012) 11 final <http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf>

16 District Court of Tel-Aviv, 49918-05-12, Amir Savir v. Google, July 5, 2015. Note on the case <https://globalfreedomofexpression.columbia.edu/cases/ami-savir-v-google-israel/> See also the California statute 'Privacy Rights for California Minors in the Digital World' (took effect as of January 1, 2015), Code § 22581(a)-(f), providing a limited right to erasure, available only to minors and only covering the information which the user posted himself or herself. Hence, content posted by third parties on the user, would not be covered.

/access. With users entrusting more sensitive information to cloud-based service providers, and hackers getting more sophisticated in their attacks on user credentials, the balance may be tipping towards stronger authentication steps. As an example, reacting to the recent theft of nude photos from individual iCloud accounts of more than 100 celebrities, reported to have been accomplished by targeted attack on user names, passwords and security questions, Apple has announced that it has expanded its use of 'two-step verification' to protect data stored on line by its customers. This apparently remains as an 'opt in' choice for the user to make.

- As long as the security setting options are clear for the user to understand and easily exercise (and the setting options include an adequate baseline of security) the user can make the trade-off between ease of use and security. Security from access by unauthorised third parties also requires a level of responsibility on the part of the user, eg, not sharing passwords and abiding by sound security practices, such as updating virus protection software, and where provided with security options, opting in to the desired security level.

Annexure

Social media platform providers – a short study

The Legal Policy & research Unit (LPRU) at the IBA London office conducted a research study for the LPD Working Group on Digital Identity on six major social media platform providers operating in diverse market segments. The LPRU screened the terms of use of these platform providers against a checklist of criteria to reflect the output in a comparative analysis table titled as Elements of Digital Identity Rights. The platform providers were: Facebook, Google+, Twitter, LinkedIn, Tuenti and WhatsApp. Tuenti, a non-US based platform provider, is based in Spain. WhatsApp is a mobile application designed to operate on smartphones and other mobile devices.

Summary note

The terms of use were easy to find in all the identified platform providers. Most of the platform providers have instructions about the use of information that is collected. All platform providers collect personal information whenever the user accesses the service, which is easily available and traceable. Movement of user information is usually controlled by the platform providers who also retain the right of disclosure of this information. The user has the right to access, amend or remove information. All platform providers incorporate the forum selection clause. Users have limited means of redress. Most of the platform providers have the right to pass information on to others.

A summary of the findings, in context with the relevant checklist questions, is provided below:

1. Are the terms of use easy to find?
The terms of use were easy to find in all the six social media platform providers.

2. Are any instructions available about the use of information that is collected by the platform provider?
Tuenti was the only platform provider where instructions were not clearly available about the use of information collected by the platform provider.

3. What / when information is collected?
Facebook collects all forms of data whenever the user interacts with the platform provider. Data is also collected from Facebook affiliates, advertising partners, location of the device and from other third parties.

Google+ collects all information given by the user and from the use of any Google services. This information is collected via cookies and anonymous identifiers.

LinkedIn collects all information when a user views and interacts with the LinkedIn pages and all related features and functions including LinkedIn mobile applications, software and platform technology. This includes IP address, browser type, mobile carrier and URLs of sites.

Tuenti collects all information that a user provides while creating a profile and whenever it is accessed by the user. Information is also collected by cookies.

Twitter collects all information that is provided upon registration and includes information collected through tweets (and metadata provided with tweets). It includes log data, widget data, data through cookies, location and data collected through third-party service providers.

WhatsApp collects all user provided information, cookie information and log file information which includes status messages and updates, time and date stamps and the mobile phone numbers the messages were sent from and to. WhatsApp also accesses address book or phone contact list available in the users mobile phone.

4. Who controls and what rights are reserved on the information?

Facebook user controls information using controls provided by Facebook under the relevant privacy and application settings. The user owns all content and information posted on Facebook and controls its sharing. Facebook also controls information given by the users and enforces its terms of use by the means it seems appropriate, but disclaims responsibility. For content that is covered by intellectual property rights (IP content), the user specifically gives Facebook a non-exclusive, transferable, sub-licensable, royalty-free, worldwide license to use any IP content that the user posts on or in connection with Facebook (IP licence).

Google+ allows the user to control the sharing of information. Google reserves the right to block or remove Google+ pages that violate the terms of service or that have been dormant for more than 9 months. Terms of service state that property rights on content submitted by the user is owned by the user, but Google is not responsible for the published information.

LinkedIn allows the user to be solely responsible for any submission of contents and interactions with other users. LinkedIn may limit and also prohibit the number of connections the user may have with other users. LinkedIn reserves the right, but has no obligation, to monitor disputes between the user and other members and to restrict, suspend, or close account which is subject to LinkedIns discretion. LinkedIn reserves all rights not expressly granted in the user agreement, including, without limitation, title, ownership and intellectual property rights.

Tuenti user is fully responsible for the information published. Tuenti reserves the right to limit published information or to deactivate or delete any profile. Upon publishing content (statuses, photos, files, text, video, sounds, drawings, logos, or any other material) on the profile, the user maintains all rights to the content and grants Tuenti a limited license to reproduce and publicly communicate it, and to add information and make necessary modifications to adapt it to the technical requirements of the service.

Twitter user retains the right to any content submitted, posted or displayed on or through the use of services offered. By submitting, posting or displaying content on or through the services, the user grants Twitter a worldwide, non-exclusive, royalty-free license (with the right to sublicense) to use, copy, reproduce, process, adapt, modify, publish, transmit, display and distribute such content in any and all media or distribution methods (now known or later developed). The license includes the right for Twitter to make content available to other companies, organisations or individuals who partner with Twitter for the syndication, broadcast, distribution or publication of such content

on other media and services. Twitter may modify or adapt the user's content in order to transmit, display or distribute it over computer networks as and when necessary.

WhatsApp user retains all user ownership rights in the status submissions, but the user has to have the rights in the first place. WhatsApp only acts as a repository of data. It is not responsible for the status information submitted through the application. However it reserves the right to remove content and status submissions without prior notice. By submitting the status submissions to WhatsApp, the user grants WhatsApp a worldwide, non-exclusive, royalty-free, sublicenseable and transferable license to use, reproduce, distribute, prepare derivative works of, display, and perform the status submissions in connection with the WhatsApp service and WhatsApps (and its successors) business, including without limitation for promoting and redistributing part or all of the service (and derivative works thereof) in any media formats and through any media channels.

5. How can the user exercise rights? In particular, (how) can the user access/amend/remove information?

Facebook user can contact Facebook by mail or through special help page to ask questions or complain about data use policy or practices. The user has the right to delete and deactivate the account. The laws of the State of California, USA, will govern the statement of rights and responsibilities, as well as any claim that might arise between the user and Facebook, without regard to conflict of law provisions. The user will have to submit to the personal jurisdiction of the courts located in Santa Clara County, California, USA for litigation purposes.

Google+ user has the right to update, rectify and delete any information provided by the user unless that information has to be kept for legitimate business or legal purposes. Google may reject requests that are unreasonably repetitive, require disproportionate technical effort, risk the privacy of others, or would be extremely impractical (for instance, requests concerning information residing on backup tapes). Where required, the laws of State of California, USA, excluding California's conflict of laws rules, are applicable to any disputes arising out of or relating to the terms or the Services. The user will have to submit to the personal jurisdiction of the courts located in Santa Clara County, California for litigation purposes.

LinkedIn user can review, enhance or edit personal information through the personal profile page; control what information is made available to search engines through the users public profile; install or remove any third party applications; control sharing of users profile information with third parties through Developer Applications installed by user connections; change profile settings to control visibility and accessibility; control LinkedIn professional plugins across the web; control how LinkedIn uses name and profile photo in social ads; and tell Linkedin to close the profile account. In case of a legal dispute any claims shall be governed by the laws of the State of California, USA, notwithstanding of any conflicts of law principles and the UN Convention for the International Sale of Goods. All claims must be resolved exclusively by a state or federal court located in Santa Clara County, California, USA. For any claim where the total amount of the award sought is less than $10,000, the party requesting relief may elect to resolve the dispute by arbitration.

Tuenti user can refuse Tuenti the right to send commercial and promotional communications, including by electronic means. The user has the right to access all personal information, to know how and why Tuenti uses it. The user can rectify any errors in personal information. Spanish law will

be applicable to resolve all disputes and the user will need to submit to the jurisdiction of courts and tribunals in the city of Madrid, Spain.

Twitter user is provided with tools and account settings rights to access or modify personal information on Twitter. The user can deactivate the account for upto 30 days and can also permanently delete the account. All claims, legal proceedings or litigation arising in connection with Twitter services will be brought solely in the federal or state courts located in San Francisco County, California, USA. The jurisdiction clauses may not apply where the user is a federal, state, or local government entity in the USA using the services in its official capacity that is legally unable to accept the controlling law, jurisdiction or venue.

WhatsApp user can decline to submit personally identifiable information through the WhatsApp site or the WhatsApp service, whereby WhatsApp may not be able to provide certain services to the user. Any cause of action must commence within one year after the accrual of the cause, otherwise the action is permanently barred. The user will be subject to the jurisdiction of State of California, USA, in the event of any legal dispute.

6. Does the platform provider have the right to pass information on to others?

Facebook has the right to pass on information on to others. But it only provides data to its advertising partners or customers after it has removed a Facebook users name or any other personally identifying information from it, or has combined it with other people's data in a way that it is no longer associated with the user. Facebook may access, preserve and share users' information in response to a legal request or to detect, prevent and address fraud and other illegal activity; to protect itself, users and others, including as part of investigations; and to prevent death or imminent bodily harm.

Google+ shares information with companies, organisations and individuals outside of Google when consent is given by user; with domain administrators; with external processing businesses and; for legal reasons including investigation of potential violations; to detect, prevent, or otherwise address fraud, security or technical issues; or to protect against harm to the rights, property or safety of users or the public as required or permitted by law.

LinkedIn users have to acknowledge, consent and agree that LinkedIn may access, preserve, and disclose registration and any other information the user provides if required to do so by law or in a good faith belief that such access preservation or disclosure is reasonably necessary in LinkedIns opinion to comply with legal process or compulsory disclosures; or if it needs to respond to claims of a violation of the rights of third parties, whether or not the third party is a user, individual, or government agency.

Tuenti does not address this question in its terms of use.

Twitter may share or disclose users' information at the user's direction (eg, when the user authorises a third-party web client or application to access information. Twitter may also share the users private personal information with service providers subject to confidentiality obligations consistent with the privacy policy, and on the condition that the third parties use the users private personal data only on Twitters behalf and pursuant to its instructions. Twitter may preserve or disclose the users information if it believes that it is reasonably necessary to comply with a law, regulation or legal request, or to protect the safety of any person or to address fraud, security or technical issues or to

protect Twitters rights or property or business transfers. It may also share or disclose users' non-private, aggregated or otherwise non-personal information.

WhatsApp can pass information on to other users about the service (eg, status submissions). It may share personally identifiable information with third party service providers, if necessary, to perform, improve or maintain the service. It may also share non-personally-identifiable information (eg, anonymous user usage data, referring / exit pages and URLs, platform types, asset views, number of clicks, etc.) with third-parties to assist them in understanding the usage patterns for certain content, services, advertisements, promotions, and/or functionality on the WhatsApp site. WhatsApp may collect and release personally identifiable and non-personally-identifiable information if required to do so by law and if necessary to comply with state and federal laws of the USA. WhatsApp also reserves the right to disclose personally identifiable and/or non-personally-identifiable information to take precautions against liability, to investigate and defend itself, or to assist government enforcement agencies in the interest of security and safety of users.

the global voice of
the legal profession®