Best Practices in Information Governance and Security

Marydee Ojala 2

Governance to Keep Private Information Private

Who doesn't have something they'd like to keep private? Maybe it was that outfit you wore to a high school dance that seemed stunning at the time, but in retrospect, not so much. You hope that no photos of it exist. Or that comment you made about the negative aspects of a neighbor's house remodeling project without realizing the neighbor could hear you. Where's that cone of silence when you need it?…

Patricia C. Franks, ... 3
San José State University

Data Privacy Regulations Versus Blockchain Technology

Data privacy refers to the use and governance of personal data, including policies implemented by businesses and governments that govern the collection, sharing and use of an individual's personal information. Information privacy refers to the individual's right to exert some control over their own personal information that is collected and used by others. These two views of privacy are reflected in legislation enacted to govern organizations and, most recently, give more power to individuals. …

Produced by:

KMWorld Magazine
Specialty Publishing Group

For information on participating in the next white paper in the "Best Practices" series, contact:

Stephen Faig
Group Sales Director
908.795.3702
sfaig@infotoday.com

LaShawn Fugate
Account Executive
859.361.0667
lashawn@infotoday.com

KMWorld
KMWorld.com

Governance to Keep Private Information Private

By Marydee Ojala, Conference Program Director, Information Today, Inc.

Marydee Ojala

Marydee Ojala is conference program director for Information Today, Inc. She works on conferences such as Enterprise Search & Discovery, which is co-located with KMWorld, and WebSearch University, among others. She is a frequent speaker at U.S. and international information professional events. In addition, she moderates the popular KMWorld webinar series.

Ojala is based in Indianapolis, Indiana and can be reached at marydee@infotoday.com.

Who doesn't have something they'd like to keep private? Maybe it was that outfit you wore to a high school dance that seemed stunning at the time, but in retrospect, not so much. You hope that no photos of it exist. Or that comment you made about the negative aspects of a neighbor's house remodeling project without realizing the neighbor could hear you. Where's that cone of silence when you need it?

Regardless of the repercussions of a bad clothing choice or the necessity to grovel while apologizing to your neighbor, other privacy matters have more severe consequences. Someone who has been cited for running a stop sign, or those falsely accused of a crime they are later proven not to have committed, have very valid reasons for wanting those actions kept private. You probably don't want your medical conditions broadcast to the world at large—or to your employer. You want the knowledge of precisely who you voted for kept secret, although you do want people to know that you did your civic duty and voted. You also don't want criminals to have access to your bank account or your credit card passwords. What about your email? You probably don't want a stranger reading your messages.

Leaks of private information can have disastrous results. In business, you might have a technology, the details of which you don't divulge because they give you a competitive advantage. Memos and reports regarding a new product launch or a strategic acquisition should be private. For public companies, early release of earnings data will attract the ire of the Securities & Exchange Commission. The resignation of the U.K. ambassador to the U.S. over leaked memos to his government is another object lesson about the importance of privacy.

There's an ongoing paradox when it comes to privacy. On the one hand, privacy matters, and individuals want their personal information to be private. On the other hand, social media, particularly Facebook and Twitter, encourage us to share information that we might otherwise keep private. A photo of your dinner plate and the awesome presentation that a wonderful restaurant has created on it is perfectly acceptable. A photo of your newly received debit card, complete with full number, your name, and the CSC code is seriously stupid.

Creating Privacy Guidelines

Within the enterprise, it's the job of the information governance team to keep private information private. Private information comprises any personal data that has been collected about individuals. That is becoming an increasingly important task, as outside legislation takes a very dim view of data breaches. Individuals' right to privacy is now codified, most stringently in the European Union's General Data Protection Regulation (GDPR). Companies and non-profit entities alike raced to be in compliance by May 25, 2018. Since GDPR took effect, more care in protecting personal data has become imperative.

> ***"There's an ongoing paradox when it comes to privacy. On the one hand, privacy matters, and individuals want their personal information to be private. On the other hand, social media, particularly Facebook and Twitter, encourage us to share information that we might otherwise keep private."***

As information governance experts know, and are at pains to inform upper management, the fact that it originated in the EU doesn't mean it is restricted to Europe. It affects all enterprises, even those outside Europe, if they have any data from EU citizens or offer goods and services to EU citizens. Other geographic entities, such as California, are looking favorably at GDPR and drafting legislation to further protect consumers.

The Role of Blockchain

What may not be as well known, says Patricia C. Franks, a professor at the School of Information at San José State University, is the role of blockchain when it comes to information governance. Blockchain, the digital ledger technology most commonly associated with cryptocurrency such as Bitcoin, is gaining ground as a means of securing data against corruption and improving efficiency in many transactions by removing the "middleman." Real estate, finance, and government are experimenting with blockchain to see if it has real business advantages.

The downside to blockchain, as Franks points out, is susceptibility to exposure of personal data. It could run counter to the basic premise of GDPR, which is the right to be forgotten, also known as the right of erasure. Data stored in digital ledgers, complete with public/private keys, digital signatures, and cryptographic hashes, should be tamper-proof. However, this also means that it can't be changed. If the data is incorrect or reveals something an individual wants erased, it's unclear how that could happen in the blockchain environment.

Franks cites the French Commission Nationale Informatique & Libertes (CNIL) as a good source for possible solutions to the data deletion dilemma posed by blockchain. CNIL explains about legislative exemptions, deleting the private key, and creating an editable blockchain. Franks recommends that, before actually deploying blockchain, an enterprise should consider the implications from a data privacy and information governance perspective. In a rapidly changing technological world, constant monitoring is called for.

Outfitting for Data Privacy

Keeping your individual data private is more under your control than ever before. Information governance is an integral part of today's business environment, and maintaining compliance with GDPR and other privacy legislative initiatives, including keeping personal data off a blockchain implementation, is key to best information governance practices.

But about that outfit you wore to the high school dance? It doesn't fall under GDPR and blockchain technology isn't keeping track of it. Hoping it is non-viewable could be completely out of your control. You may just have to grin and bear it, sorry to say. ▮

Data Privacy Regulations Versus Blockchain Technology

By Patricia C. Franks, Professor, School of Information at San José State University

Data privacy refers to the use and governance of personal data, including policies implemented by businesses and governments that govern the collection, sharing and use of an individual's personal information. Information privacy refers to the individual's right to exert some control over their own personal information that is collected and used by others. These two views of privacy are reflected in legislation enacted to govern organizations and, most recently, give more power to individuals.

EU's General Data Protection Regulation

The European Union's General Data Protection Regulation (GDPR), which took effect on May 25, 2018, is a comprehensive regulation that includes provisions for client consent, data breaches, data processing, security, and individual subject rights. It was designed to protect the privacy rights and freedoms of EU citizens and harmonize data privacy laws across all twenty-eight EU member states.

The GDPR applies to all companies processing the personal data of data subjects residing in the EU, regardless of a company's location. It also applies to the processing of personal data of data subjects in the EU by a controller or processor not established in the EU, where the activities relate to offering goods or services to EU citizens (irrespective of whether payment is required) and the monitoring of behavior that takes place within the EU.

One provision of the GDPR that can be problematic for companies employing blockchain technology is the right to be forgotten (i.e., the right of erasure).

Data Privacy in the United States

There is no single principal data protection legislation in the U.S. Hundreds of laws enacted on the federal and state levels attempt to protect the personal data of U.S. residents and often apply to specific industry sectors such as financial services, healthcare, telecommunications, and education. One example of U.S. federal data protection laws is The Federal Trade Commission Act (15 U.S. Code § 41 *et seq.)*, which enforces actions against companies for failing to comply with their own posted privacy policies and for disclosing personal data without authorization. A second example is The Health Insurance Portability and Accountability Act (HIPAA) 42 U.S.C. §1301 *et. seq.*), which regulates medical information by entities that handle the information, including healthcare providers, data processors, and pharmacies.

Privacy rights not granted by the federal government are left to individual states to protect. The *California Consumer Privacy Act (CCPA)*, passed into California law on June 28, 2018, is the strongest data privacy legislation enacted in the U.S. to date and closely mirrors the GDPR. It requires businesses to disclose the purpose for the information collected or sold, as well as the third-party organizations receiving the data. It gives consumers the right to ask businesses for the types and categories of personal information being collected, as well as the right to request data be deleted and to initiate civil action if they believe that an organization has failed to protect their personal data.

Blockchain Technology

In their 2016 book, *Blockchain Revolution*, Don & Alex Tapscott defined blockchain as "an *incorruptible [immutable] digital ledger* of *economic transactions* that can be programmed to record not just financial transactions but virtually *everything of value*" (Tapscott, 2016).

When data is stored in a digital ledger using public/private keys, digital signatures, and cryptographic hashes—tampering is immediately obvious. The append-only data store secures against deletion or alteration and, therefore, is a useful data structure for storing audit data.

Before deploying blockchain technologies, organizations must determine whether the implementation is consistent with data privacy regulations. Understanding whether blockchain implementations promote privacy objectives or undermine these objectives is an important consideration.

Organizations under the jurisdiction of the GDPR and CCPA, or similar legislation, should proceed with caution before storing personal data on a blockchain. The immutable nature of blockchain technology provides challenges to organizations faced with right to erasure and correction requests.

Patricia C. Franks

Patricia C. Franks, a professor for the School of Information at San José State University, coordinates the Master's degree in Archives and Records Administration (MARA). She holds a doctorate/Ph.D. in Organization and Management and is a Certified Archivist (CA), Certified Records Manager (CRM), an Information Governance Professional (IGP), and a member of ARMA International's Company of Fellows. She is author of the book *Records and Information Management* (2013, 2018).

The CNIL (Commission Nationale Informatique & Libertes) notes that it is "technically impossible to grant the request for erasure made by a data subject when data is registered on a blockchain" (CNIL, n.d., p. 8). Methods to delete data from a blockchain are not available, but this may change. Several solutions to this dilemma have been posed:

1. **Exemption:** Some believe that legislation that provides an exemption for personal data stored on a blockchain may be the answer.
2. **Deletion of the private key:** This is a technical means to render encrypted data unusable by deleting the keyed hash function's secret key. This will make it impossible to prove/verify which information was hashed but may not satisfy the requirements of the legislation.
3. **An editable blockchain:** In 2016, Accenture was awarded a patent for an "editable blockchain" for enterprise use. While geared to permissioned (privately controlled) blockchains, this option could allow organizations to alter data in the event of errors or fraud—and possibly to respond to requests to erase private information.

Conclusion

For now, if your organization employs blockchain technology, the best way to ensure compliance with privacy regulations such as GDPR, CCPA, and similar legislation is to keep personal data off the blockchain. The feasibility of deploying a solution that links to data off the blockchain will depend on how well the blockchain technology employed integrates with existing enterprise systems. However, the speed at which both blockchain technology and legislation are evolving requires constant monitoring of both. ▮

References

Commission Nationale Informatique & Libertés (CNIL). n.d. *Blockchain: Solutions for responsible use of the blockchain the context of personal data* (p.8). Paris, France: CNIL.

Tapscott, Don and Alex. (2016). *Blockchain Revolution*. Old Tappan, New Jersey: Penguin Group (USA) LLC).

For more information on the companies who contributed to this white paper, visit their websites or contact them directly:

SJSU SAN JOSÉ STATE UNIVERSITY

San José State University
School of Information
One Washington Square
San José, CA 95192-0029
Phone: (408) 924-2490
Contact: ischool@sjsu.edu
Website: https://ischool.sjsu.edu

Produced by:

KMWorld Magazine
Specialty Publishing Group

Stephen Faig
Group Sales Director
908.795.3702
sfaig@infotoday.com

LaShawn Fugate
Account Executive
859.361.0667
lashawn@infotoday.com

For information on participating in the next white paper in the "Best Practices" series, contact:
sfaig@infotoday.com | 908.795.3702 | lashawn@infotoday.com | 859.361.0667

KMWorld
www.kmworld.com

Information Today, Inc.
www.infotoday.com