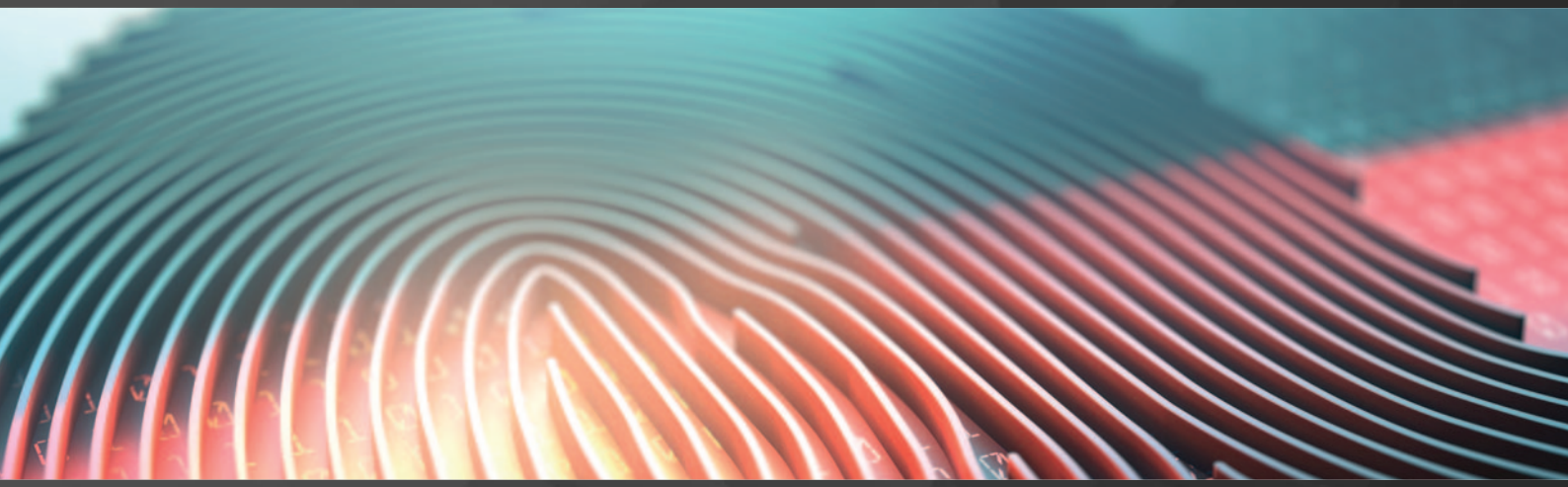
International Comparative Legal Guides



Cybersecurity 2020

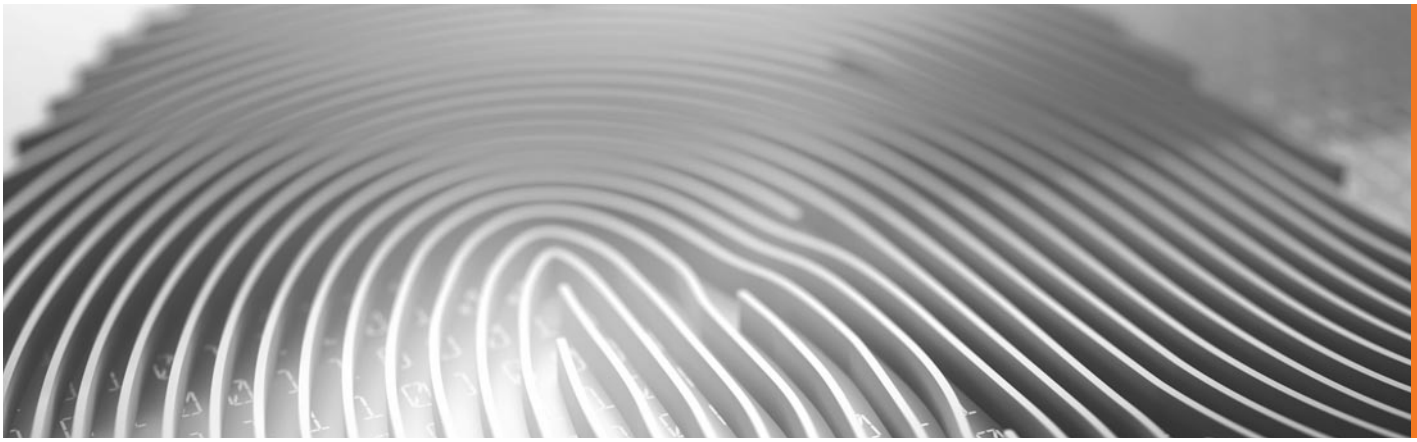
A practical cross-border insight into cybersecurity law

Third Edition

Featuring contributions from:

Advokatfirmaet Thommessen AS
Allen & Overy LLP
Boga & Associates
Christopher & Lee Ong
Cliffe Dekker Hofmeyr
Creel, García-Cuéllar, Aiza y Enríquez, S.C.
Eversheds Sutherland
Faegre Baker Daniels
G+P Law Firm
Gikera & Vadgama Advocates
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.
Iwata Godo
King & Wood Mallesons
Lee & Ko
Lee and Li, Attorneys-at-Law
LEĜA
Lesniewski Borkiewicz & Partners (LB&P)
Maples Group
McMillan
Mori Hamada & Matsumoto
Niederer Kraft Frey Ltd.
Nyman Gibson Miralis
Pearl Cohen Zedek Latzer Baratz
R&T Asia (Thailand) Limited
Rajah & Tann Singapore LLP
Ropes & Gray
SAMANIEGO LAW
Shardul Amarchand Mangaldas & Co.
Siqueira Castro – Advogados
Sirius Legal
Stehlin & Associés
Synch

ICLG.com



ISBN 978-1-83918-005-7
ISSN 2515-4206

Published by
global legal group
59 Tanner Street
London SE1 3PL
United Kingdom
+44 207 367 0720
www.iclg.com

Group Publisher
Rory Smith

Associate Publisher
James Strode

Senior Editors
Caroline Oakley
Rachel Williams

Deputy Editor
Hollie Parker

Creative Director
Fraser Allan

Printed by
Stephens & George
Print Group

Cover Image
www.istockphoto.com

Cybersecurity 2020

Third Edition

Contributing Editors:
Nigel Parker and Alexandra Rendell
Allen & Overy LLP

Strategic Partners

Expert Chapters

1 **Effective Cyber Diligence – The Importance of Getting it Right**
Nigel Parker & Alexandra Rendell, Allen & Overy LLP

4 **Franchising in a Sea of Data and a Tempest of Legal Change**
Paul Luehr, Huw Beverley-Smith, Nick Rotchadl & Brian Schnell, Faegre Baker Daniels

11 **Why AI is the Future of Cybersecurity**
Akira Matsuda & Hiroki Fujita, Iwata Godo

Country Q&A Chapters

15 **Albania**
Boga & Associates: Genc Boga & Armando Bode

21 **Australia**
Nyman Gibson Miralis: Dennis Miralis, Phillip Gibson & Jasmina Ceic

29 **Belgium**
Sirius Legal: Roeland Lembrechts & Bart Van den Brande

37 **Brazil**
Siqueira Castro – Advogados:
Daniel Pitanga Bastos De Souza & João Daniel Rassi

43 **Canada**
McMillan: Lyndsay A. Wasser & Kristen Pennington

51 **China**
King & Wood Mallesons: Susan Ning & Han Wu

59 **Denmark**
Synch Advokatpartnerselskab: Niels Dahl-Nielsen & Daniel Kiil

66 **England & Wales**
Allen & Overy LLP: Nigel Parker & Alexandra Rendell

75 **France**
Stehlin & Associés: Frédéric Lecomte & Mélina Charlot

82 **Germany**
Eversheds Sutherland: Dr. Alexander Niethammer & Constantin Herfurth

89 **Greece**
G+P Law Firm: Ioannis Giannakakis & Stefanos Vitoratos

97 **India**
Shardul Amarchand Mangaldas & Co.:
GV Anand Bhushan, Tejas Karia & Shahana Chatterji

106 **Ireland**
Maples Group: Kevin Harnett

115 **Israel**
Pearl Cohen Zedek Latzer Baratz: Haim Ravia & Dotan Hammer

122 **Japan**
Mori Hamada & Matsumoto: Hiromi Hayashi

130 **Kenya**
Gikera & Vadgama Advocates: Hazel Okoth & Stella Ojango

137 **Korea**
Lee & Ko: Hwan Kyoung Ko & Kyung Min Son

144 **Kosovo**
Boga & Associates: Renata Leka & Delvina Nallbani

150 **Malaysia**
Christopher & Lee Ong: Deepak Pillai & Yong Shih Han

159 **Mexico**
Creel, García-Cuéllar, Aiza y Enríquez, S.C.:
Begoña Cancino

165 **Norway**
Advokatfirmaet Thommessen AS:
Christopher Sparre-Enger Clausen & Uros Tosinovic

172 **Poland**
Lesniewski Borkiewicz & Partners (LB&P):
Mateusz Borkiewicz, Grzegorz Lesniewski & Joanna Szumilo

180 **Portugal**
Gouveia Pereira, Costa Freitas & Associados, Sociedade de Advogados, S.P., R.L.: Catarina Costa Ramos

186 **Singapore**
Rajah & Tann Singapore LLP: Rajesh Sreenivasan, Justin Lee & Yu Peiyi

194 **South Africa**
Cliffe Dekker Hofmeyr: Fatima Ameer-Mia, Christoff Pienaar & Nikita Kekana

202 **Spain**
SAMANIEGO LAW: Javier Fernández-Samaniego & Gonzalo Hierro Viéitez

208 **Sweden**
Synch Advokat: Anders Hellström & Erik Myrberg

216 **Switzerland**
Niederer Kraft Frey Ltd.: Clara-Ann Gordon & Dr. András Gurovits

223 **Taiwan**
Lee and Li, Attorneys-at-Law: Ken-Ying Tseng

230 **Thailand**
R&T Asia (Thailand) Limited: Supawat Srirungruang & Visitsak Arunsuratpakdee

238 **USA**
Ropes & Gray: Edward R. McNicholas & Kevin J. Angle

246 **Venezuela**
LEĜA: Carlos Dominguez & Hildamar Fernandez

ICLG.com

From the Publisher

Dear Reader,

Welcome to the third edition of *The International Comparative Legal Guide to Cybersecurity*, published by Global Legal Group.

This publication, which is also available at www.iclg.com, provides corporate counsel and international practitioners with comprehensive jurisdiction-by-jurisdiction guidance to cybersecurity laws and regulations around the world.

This year, there are three general chapters which provide an overview of key issues affecting cybersecurity, particularly from the perspective of a multi-jurisdictional transaction.

The question and answer chapters, which cover 32 jurisdictions in this edition, provide detailed answers to common questions raised by professionals dealing with cybersecurity laws and regulations.

As always, this publication has been written by leading cybersecurity lawyers and industry specialists, to whom the editors and publishers are extremely grateful for their invaluable contributions.

Global Legal Group would also like to extend special thanks to contributing editors Nigel Parker and Alexandra Rendell of Allen & Overy LLP for their leadership, support and expertise in bringing this project to fruition.

Rory Smith
Group Publisher
Global Legal Group

Why AI is the Future of Cybersecurity


Akira Matsuda


Hiroki Fujita

Iwata Godo

Overview Surrounding Cybersecurity

What is Cybersecurity?

Cybersecurity is defined as the "*preservation of confidentiality, integrity and availability of information in the Cyberspace*" in Article 4.20 of ISO/IEC 27032:2012.

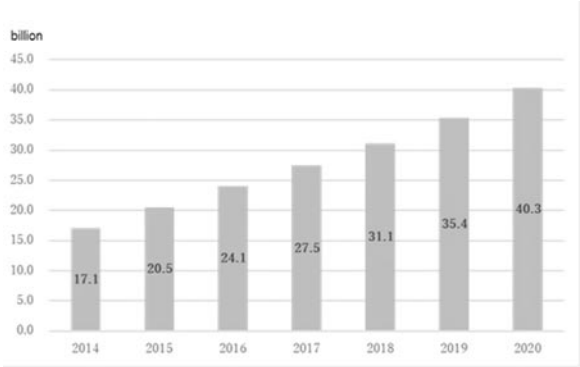
Furthermore, the cyberspace is defined as a "*complex environment resulting from the interaction of people, software and services on the Internet by means of technology devices and networks connected to it, which does not exist in any physical form*" in Article 4.21 of ISO/IEC 27032:2012.

Threats in cyberspace

As internet access becomes more pervasive across the world and IoT devices become increasingly common and cyberspace expands rapidly, the number of cyberattacks continues to grow. While an expanding cyberspace can be of great benefit to the public, the malicious use of cyberspace can result in significant economic and social losses. In cyberspace, cyber attackers have an asymmetric advantage over defenders. In particular, if defenders lag behind cyber attackers in terms of technology or defence systems, this advantage is likely to be enhanced. Unlike cyber attackers, it is difficult for defenders to introduce a new trial technology because the defenders' main role is to ensure the stability of the defence systems which could be potentially harmed and undermined by the new trial technology.

Expansion of cyberspace

Along with technological development, cyberspace keeps growing. For example, there were globally 27.5 billion IoT devices active in cyberspace in 2017, and it is estimated that this number will reach about 40 billion by 2020.[1]



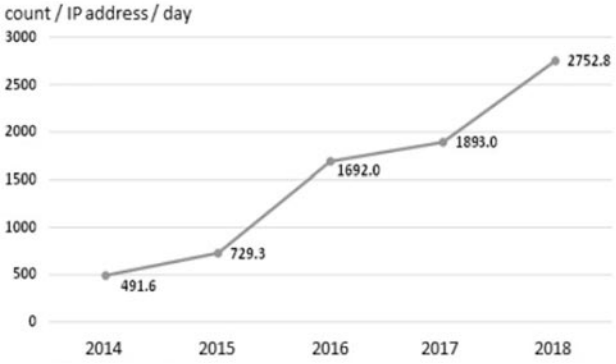
Note: The data is from "Cybersecurity 2019" by National center of Incident readiness and Strategy for Cybersecurity of Japan

The governments of many countries share the view that digitalisation is transforming every aspect of our economies and societies. The data is increasingly becoming an important source of economic growth, and its effective use should contribute to social well-being around the world. In order to facilitate this process, the "Osaka Track" framework aimed at promoting international policy discussions and the drafting of international rules to enable the free movement of data across borders (international rules on trade-related aspects of electronic commerce at the WTO) with Japan intending to be a key player, was launched on 28 June 2019.

Threats in cyberspace

As cyberspace keeps growing, the frequency of cyber attacks is increasing as a global trend. For example, in Japan, the number of unexpected connection attempts detected by the National Police Agency has risen to 2,752.8 per IP address per day in 2018.

Number of unexpected connection attempts detected by the National Police Agency of Japan



Note: From "Threats in Cyberspace 2018" by the National Police Agency of Japan.

New technologies and services, such as AI and IoT, could bring about substantial benefits to the society of the future as a society in which new values and services are created continuously, making people's lives more conformable and sustainable. On the other hand, there is a growing concern that these technologies could also be used in malicious ways. The risk is that users and providers of AI or IoT related services will not be able to sufficiently and adequately control these technological developments and their use. With the growth of cyberspace, new threats are emerging and also as to their scale, scope, and frequency and threats are escalating as more sophisticated and organised attackers are designing targeted attacks to damage or disrupt critical infrastructures and services. These disruptions can have a huge financial impact or paralyse vital activities. Cyberattacks can generally lead to loss of money, theft of

personal information/identity/IP, and damage to reputation and safety, cause problems with business services, transportation, health and power.

For example, the Central Bank of Bangladesh was hacked in December 2015, resulting in the embezzlement of about US$ 81 million, and a state-owned power company substation was attacked in December 2016 in Ukraine, resulting in a one-hour blackout. In Japan, cyber attacks have been successfully conducted to steal crypto assets in 2018.

Superiority of cyber attackers

Cyberspace is a place where everyone can utilise new information and communication technology without being constrained by location and time. A Cyber attacker has the decisive advantage as he can easily copy and disseminate data and information, including computer viruses/malware, and can flexibly use advanced technologies such as AI and blockchain. In contrast, it is generally difficult for defenders to respond to cyber attacks because the resources they can use are limited, no defensive capability remains indefinitely effective and they are forced to respond with their then currently existing systems and technologies to ensure the stability and resilience of their defence system. Unlike Cyber attackers, it is difficult for defenders to introduce a new trial technology because the new trial technology can harm or undermine the stability of defence systems. In addition, it is impossible to completely eliminate vulnerabilities caused by human errors linked to the use of information systems, so that many cyber attacks involve looking for weaknesses in user behaviour that can be exploited through seemingly legitimate means (so-called "social hacking/social engineering").

Countermeasures

As cyber attacks are spreading in Cyberspace, where attackers seem to have a constant decisive advantage over defenders and their ability to assess and address risks, "Active Cyber Defense" can be considered to be an effective countermeasure to such cyberattacks. Having an "Active Cyber Defense" means that the organisation proactively protects itself in advance rather than responding to a cyber attack which has occurred. In Japan, for example, the Ministry of Internal Affairs and Communications, which is the national watchdog in charge of cybersecurity-related laws and regulations, and the National Institute of Information and Communications Technology, which researches and promotes information and communications technology, have collaborated with internet service providers to launch the "NOTICE" program designed to investigate IoT devices which might be misused/hacked in cyber attacks because of weak authentification mechanisms (IDs and passwords), and to alert users. We understand that similar objectives are being pursued in many other countries.

To organise an "Active Cyber Defense", the utilisation of AI is considered to be very important. This is because Cyber attackers always use new offensive tools to conduct cyber attacks, so that, in order to respond to cyber attacks effectively, detection and analysis by AI are necessary. AI technology can be used to track new patterns or offensive strategies which could otherwise not be detected without machine learning mechanisms. In addition, by introducing AI in their defence strategy, humans can focus on their analysis of causes and impact at the time of a cyber attack and as the case may be react to false detection. It is possible to increase the efficiency and accuracy of defence systems in cyberspace but to stay one step ahead is challenging.

Relationships Between Cybersecurity and AI

Trends/directions followed by AI utilisation

As for the direction of AI utilisation, as a general principle, there is a common understanding that it is extremely important not to excessively rely on AI and that humans should keep some control over the use of AI and AI-generated results and output. Ethics and morality would be negatively impacted by the excessive use of, and total dependence on, the use of AI. At this stage, many governments or integrated areas want to provide directions and guidance for the use of AI by issuing guidelines. For example, the "Principles for a Human-centric AI Society" were published in March 2019 in Japan and "Ethics Guidelines for Trustworthy AI" was published by the European Commission in April 2019.

Relationship between Cybersecurity and AI

The globally accepted and prevalent categorisation of the relationships between Cybersecurity and AI is the following and can be divided into four categories: "Attacks using AI"; "Autonomous attacks by AI"; "Attacks against AI"; and "Security measures using AI".

Attacks using AI

Cyber attackers use AI for cyber attacks. Such attacks are actually occurring in the real world.

Autonomous attacks by AI

AI performs cyber attacks autonomously without human intervention. However, under the current AI model, this category is not yet in existence. Once it becomes technically possible for AI to perform cyber attacks autonomously without human intervention, one difficulty will be to allocate responsibility as regards civil damages caused by cyber attacks.

Attacks against AI

This category covers cyber attacks against AI and the so-called "Adversarial Learning"; for example, where a cyber attacker may feed fake data to AI. Such an attack could become realistic in the future if human involvement in AI monitoring declines and the use of AI for critical decisions (such as diagnostics and investment decisions, etc.) becomes general.

Security measures using AI

This category covers defenders using AI against cyber attacks. Various attempts have already been made, such as the automation of malware detection. At present, human beings continue to be responsible for determining those issues to be solved by AI and interpreting decisions by AI. Therefore, it is necessary to develop human resources that can fully utilise AI.

We will discuss "Security measures using AI" further in detail below.

Security Measures Using AI

Benefits of using AI

There are four benefits of using AI for Cybersecurity:

Reducing the cost of detection and response to breaches

Using AI for cybersecurity enables organisations to understand and reuse threat patterns to identify new threats. This leads to an overall reduction in time and effort to identify threats and incidents, investigate them, and remediate incidents.

Becoming faster at responding to breaches

A fast response is essential to protect an organisation from cyber attacks. According to the 2019 Capgemini's Reinventing Cybersecurity with Artificial Intelligence Report, using AI for cybersecurity, the overall time taken to detect threats and breaches is reduced by up to 12% and the time taken to remediate a breach or implement patches in response to an attack is also reduced by 12%. A small subset of organisations even managed to reduce these time metrics by more than 15%.

Increasing efficiency

Cyber analysts spend considerable time going through data logs and/or incident timesheets. Notwithstanding the significant workforce involved in cybersecurity, cyber analysts with deep knowledge of this field are rare. By using good data to analyse potential threats, AI enables cyber analysts to focus on works which only humans can do, such as analysing the incidents identified by the AI cybersecurity algorithms.

Making new revenue streams

As mentioned above, with the proliferation of IoT devices, the number, scope and scale of attacks has significantly increased. This creates opportunities for vendors offering cybersecurity services to manufacturers of IoT devices. Many players are taking advantage of the huge market opportunities.

Present Status of security measures using AI

As mentioned above, there are a lot of benefits to use AI for cybersecurity purposes, but at present AI can only be used to assist human work conducted for the purpose of cybersecurity, and human involvement is necessary. In other words, it is still necessary for human beings to continue to be responsible for customising teacher data to be learned by AI, determining issues to be solved by AI, and interpreting AI decisions.

In addition, decisions by AI use the "black box" model that lacks transparency as providing only input-output without the underlying rationale, and it is difficult to determine why the decision has been made. White-box models are the type of models which one can clearly explain how they behave and produce predictions and what the influencing variables are. However, they are yet to be put into practical use.

Security Measures Using AI and Fiduciary Duty of Care

Fiduciary duty of care

In many jurisdictions, directors and officers (hereinafter officers) of a company owe a fiduciary duty of care to the company. If an officer breaches a fiduciary duty of care in performing his/her role, the officer is liable to the company for the damage caused as a result.

Can it be considered that officers appropriately fulfil their fiduciary duty of care by introducing AI for cybersecurity purposes?

Use of AI for security measures and performance of fiduciary duty of care

As mentioned above, there are still some technical hurdles before AI can be used for security measures at present so that the introduction of AI itself in corporate procedures and strategies does not necessarily mean that the officer in charge of cybersecurity is appropriately discharging his/her duty and can be exculpated. Fairly common standards for determining the existence of a breach of fiduciary duty apply in many jurisdictions: whether the fiduciary duty of care is appropriately fulfilled is determined based on what would be normally expected from an ordinary officer having reasonable skills, experience and knowledge in a company of the same size and industry. Therefore, the introduction of AI does not necessarily mean that officers appropriately fulfilled their fiduciary duty of care under the present state of the art where it is clear that adequate and sufficient cybersecurity protection cannot be achieved through the mere introduction of the AI without appropriate human intervention and monitoring. Unless comprehensive security measures such as appropriate human intervention and human decision-making are introduced, cybersecurity measures could be determined to be insufficient. Accordingly, it is important for officers to build comprehensive cybersecurity system framework, and AI could be used to achieve this purpose as a part of structuring the cybersecurity system.

However, once these AI issues are resolved and the mere introduction of an AI-based cybersecurity system is widely recognised as appropriate for the cybersecurity protection of the company, it may be possible that an officer will be deemed to perform his fiduciary duty of care by simply introducing the appropriate AI-based cybersecurity system. If the absence of an AI-based cybersecurity system becomes a negative factor in the determination of a breach of fiduciary duty of care, it will be an incentive for all officers to introduce AI.

Future Prospects

As mentioned above, AI still has a lot of issues to overcome to form a stand-alone cybersecurity system. However, even at this early stage, in light of the benefits which could be derived from its use, AI will become an unavoidable tool in any efficient cyber defence strategy (especially where AI is being used in the attack).

The 2020 Tokyo Olympics and the 2025 World Exposition to be held in Japan are obvious targets. Major events have become attractive targets for "hacktivists" and fraudsters. The Rio de Janeiro Olympics in 2016 and the Pyeongchang Olympics in 2018 have been under heavy attacks (with allegations of cyberwarfare).

Cybersecurity is a hot topic and will be so for the years to come. Every state, business and individual will need to remain wary and watchful: no doubt AI will help.

Endnote

1. National center of Incident Readiness and Strategy for Cybersecurity, *Cybersecurity 2019*, May 23rd, 2019.

Akira Matsuda is an attorney-at-law (admitted in Japan and New York) and a partner at Iwata Godo heading the AI/TMT and Data Protection practice group. He is based in Tokyo and Singapore. His practice focuses on cross-border transactions, including mergers and acquisitions, as well as international disputes (litigation/arbitration), and advice on digital/TMT related matters. Mr. Matsuda regularly advises Japanese and foreign clients on data security issues (Japanese laws, Singapore PDPA, and EU GDPR) including on the structuring of global compliance systems. He also advises complicated cross-border corporate investigation matters.
He is a graduate of the University of Tokyo (LL.B.) and Columbia Law School (LL.M.).

Iwata Godo
Marunouchi Building 10F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6310
Japan

Tel: +81 3 3214 6205
Email: amatsuda@iwatagodo.com
URL: www.iwatagodo.com

Hiroki Fujita is an attorney-at-law (admitted in Japan) and associate at Iwata Godo. He is a member of the firm's AI/TMT and Data Protection practice group. His practice focuses on intellectual property law and IT. Mr. Fujita regularly advises clients across a broad range of industries, including electric power utilities and telecom carriers on data protection and cybersecurity issues. Mr. Fujita also advises clients on corporate matters, including mergers and acquisitions and corporate disputes (litigation/arbitration).
He is a graduate of Osaka University (LL.B.) and the Kyoto University School of Law (JD).

Iwata Godo
Marunouchi Building 10F
2-4-1 Marunouchi
Chiyoda-ku
Tokyo 100-6310
Japan

Tel: +81 3 3214 6205
Email: hiroki.fujita@iwatagodo.com
URL: www.iwatagodo.com

Iwata Godo is one of Japan's premier and oldest law firms. It was established in 1902 as one of the first business law firms by Chuzo Iwata, an attorney-at-law who subsequently held various positions, including serving as Minister of Justice and president of the Japan Federation of Bar Associations. It is a full-service firm with about 70 attorneys and each of its practice areas is highly regarded. It is the firm of choice for clients with respect to their most challenging legal issues, including in relation to data protection. Over the past few years, Iwata Godo has hosted a number of international seminars and conferences on data protection, often in coordination with "best friend" firms that are renowned firms and market leaders in their jurisdictions.

www.iwatagodo.com

IWATA GODO
Established 1902

ICLG.com

Current titles in the ICLG series

Alternative Investment Funds
Anti-Money Laundering
Aviation Law
Business Crime
Cartels & Leniency
Class and Group Actions
Competition Litigation
Construction & Engineering Law
Copyright
Corporate Governance
Corporate Immigration
Corporate Investigations
Corporate Recovery & Insolvency
Corporate Tax
Cybersecurity
Data Protection
Employment & Labour Law
Enforcement of Foreign Judgments
Environment & Climate Change Law
Family Law
Financial Services Disputes
Fintech
Foreign Direct Investments
Franchise
Gambling
Insurance & Reinsurance
International Arbitration
Investor-State Arbitration
Lending & Secured Finance
Litigation & Dispute Resolution
Merger Control
Mergers & Acquisitions
Mining Law
Oil & Gas Regulation
Outsourcing
Patents
Pharmaceutical Advertising
Private Client
Private Equity
Product Liability
Project Finance
Public Investment Funds
Public Procurement
Real Estate
Sanctions
Securitisation
Shipping Law
Telecoms, Media and Internet Laws
Trade Marks
Vertical Agreements and Dominant Firms

@ICLG_GLG

The International Comparative Legal Guides are published by global legal group