REPRISK®
ESG Business Intelligence

GEC Risk Advisory
Transforming Risk into Value®

RepRisk and GEC Risk Advisory

Joint Special Report on Privacy Issues

July 2015

Foreword from RepRisk CEO

I am pleased to introduce our Special Report on Privacy Issues, our first joint report with our partner, GEC Risk Advisory.

The right to privacy is widely considered a human right, and the invasion of a person's privacy can raise both legal and ethical issues. Companies worldwide need to evaluate the benefits of gaining personal information on clients, employees, and the general public, against the potential damages caused by loss of reputation, and possible legal and regulatory repercussions.

This report presents case studies on different types of privacy issues, together with an analysis of how these violations could affect the companies involved. In some cases, privacy issues have prompted individuals to take legal action against the person or entity that facilitated the intrusion.

The aim of the report is to highlight the areas in which the increased use of technology has created new privacy concerns for both employers and employees, and we encourage companies to pay particular attention to privacy issues in their own operations.

Philipp Aeby
CEO, RepRisk AG

Foreword from GEC Risk Advisory CEO

In this first of what we plan to be a periodic white paper collaboration between GEC Risk Advisory and our strategic partner, RepRisk AG, we focus on the critically important topic of privacy and data breaches on a global scale – with examples from Korea, the US, Sweden, China, and Japan. Never was an issue as global and as local at the same time, with serious and complicated implications for global actors – be they corporations, non-profits, academia and even governments.

In this collaboration between GEC Risk Advisory and RepRisk, we will make use of the best of both worlds: the world of big data analytics and metrics from RepRisk, and the practical and interpretive lens of GEC Risk Advisory, with the goal of providing general takeaways from each case study.

Together, we hope to broach future important topics to multinationals and other organizations in order to help both the actors in these situations as well as their stakeholders to gain a better and more constructive understanding about how to deal with the complex ESG issues in this age of hyper-transparency and super-connectivity.

Andrea Bonime-Blanc
CEO, GEC Risk Advisory

Contents

Produced by RepRisk AG and GEC Risk Advisory

Authors: Andrea Bonime-Blanc (GEC Risk Advisory); Stella Kenway (RepRisk AG)

Editors: Alexandra Mihailescu Cichon, Gina Walser (RepRisk AG); Robin Scott (Robin Scott Translations)

Graphic Design: Bounford.com

RepRisk AG, Stampfenbachstrasse 42, 8006 Zurich, Switzerland. Tel. +41 43 300 54 40 www.reprisk.com
and
GEC Risk Advisory LLC, P.O. Box 231351, New York, New York, 10023 USA, Tel. +1 917 848 4448 www.GECRisk.com

Introduction

This Joint Special Report on privacy issues outlines the following six case studies from around the world, with the aim of highlighting areas in which an increased use of technology has created new privacy concerns for employers, employees and other stakeholders.

Each case study highlights a different type of privacy concern and was taken from the RepRisk ESG Risk Platform, a comprehensive online risk database focused on environmental, social, and governances (ESG) issues. Each risk incident presented was captured and analyzed as part of RepRisk's systematic and dynamic research process, which is based on big data from a broad range of media and stakeholder sources in 15 languages.

Each case study has two components: The first is a summary of the risk incident provided by RepRisk. The second is a practical and interpretative analysis on how these risks could affect corporates and organizations, provided by GEC Risk Advisory.

Case study	Company	Country	Sector	Issue
#1	Korea Exchange Bank	Korea	Banks	Employer monitoring employees
#2	Uber Technologies	China	Software and Computer Services	Leaked customer data sold on internet
#3	Burger King	Sweden	Travel and Leisure	Alleged spying on customers
#4	Apple, Yelp, Electronic Arts, Twitter, Instagram, Rovio, and other app developers	United States of America	Software and Computer Services	Corporate data mining
#5	Hitachi, NEC, and UBIC	Japan	Technology Hardware and Equipment; Software and Computer Services	Monitoring of employees with artificial intelligence
#6	Anthem	United States of America	Insurance	Hacking of patient information

Case 1 KEB criticized for asking employees to sign Personal Information Collection Agreement

Company: Korea Exchange Bank
Country: Korea
Sector: Banks
Issue: Employer monitors employees

RepRisk Incident: May 2015, originally reported in a Korean-language source

Employees of the Korea Exchange Bank (KEB) have expressed concerns about the Personal Information Collection Agreement that the company recently asked them to sign. Allegedly, the agreement required them to provide information about their medical history and union activities, and authorized KEB to use CCTV to monitor employees' arrival and departures times. The Agreement reportedly stated that employees who did not sign could be subjected to disadvantageous labor conditions. Many employees are concerned that the agreement might be used to suppress union activities against the merger of KEB and Hana Bank [Note: The merger was proposed when Hana Financial Group acquired KEB]. They also expressed concern about how the Agreement would be used and warned that it could be linked to privacy violations as well as monitoring and discrimination at work.

GEC Risk Analysis:

This story reflects a trend that is taking place across many businesses, especially in developed, industrialized countries where, increasingly, employers collect personal data from employees and other stakeholders, such as customers, to manage and organize the workplace and the business, or even for potentially more nefarious reasons, as this story seems to imply.

What is different about this particular case is that the company is allegedly not using big data analytics quietly in the background, but instead apparently asking employees directly to share their personal information with the company via a written agreement, which in turn may violate privacy and other laws. The fact that there is a possible merger may also be a driver of the request to sign this agreement.

In this case, there seem to be additional serious allegations of possible discrimination and labor law violations as employees claim that their livelihoods may be in jeopardy if they refuse to sign these agreements.

Key takeaways:

It is critically important that all parties understand that modern technology is rapidly changing the legal landscape, often in unpredictable ways. Companies, employees, and other stakeholders with respect to privacy issues should understand their rights and obligations wherever they are located, and be aware of whatever means are used to collect such data.

For legal reasons, an organization needs to achieve the delicate balance between the protection of individual privacy rights and the use of data to manage their business. This is true whether the request for personal information is done through traditional means (such as the Personal Information Collection Agreement alluded to here) or increasingly pervasive new means such as those employed in big data technologies.

The following are several criteria that companies and individuals should consider:

- What are the privacy laws in the jurisdictions in which they do business or work?
- How vigilant and responsive are privacy regulators or government agencies in a particular jurisdiction or country?
- How predictable and consistent is enforcement of privacy laws against corporate and other violators?
- What is the culture, leadership and tone from the top of a particular company and its executives: Does it favor privacy protection and allow for a "safe to speak up" corporate culture, or does the culture not favor transparency and the ability to "voice concerns" without fear of retaliation?

Case 2 Information on users of Uber taxis in China reported being sold via Darknet

Company: Uber Technologies
Country: China
Sector: Software and Computer Services
Issue: Leaked customer data sold on internet

RepRisk Incident: May 2015, originally reported in a Chinese-language source

Leaked information about users of the taxi service provided by Uber Technologies (Uber) in several Chinese cities has reportedly been sold on the Internet. In March 2015, there were also allegations that the company's user account information was being sold over the Darknet [Note: a private computer network based on non-standard protocols and ports]. In the US, Uber's database was apparently compromised in May 2014, which exposed the personal information of around 50,000 registered drivers to potential theft. In recent months, the legal status of Uber has been challenged in several countries and regions, including the US, China, Japan, South Korea, and Europe.

GEC Risk Analysis:

Uber has dealt with a wide variety of challenges around the world since it became a well-known and transformational brand in the transportation services business. On the one hand, it has revolutionized how people get around in just about every major urban center globally via the use of a very simple but powerful app. On the other hand, it has suffered from a variety of media exposures and reputational challenges, some of which have been self-inflicted, and some of which are due to the times in which we live.

The age of hyper-transparency and super-connectivity sometimes rewards and sometimes harms highly-visible companies. This places companies like Uber in the crossfire of the media, interest groups, regulators, and others.

Key takeaways:

Some of the issues that Uber or any other company in a similar position should be considering, based on a fact pattern similar to this one, should include the following:

- Does the company have a clear understanding of all privacy laws in jurisdictions in which it does business?
- Does the company have the right cyber-defenses and programs in place to properly protect the private information of customers?
- Is there a customer, driver, or other customer phone or other form of digital communication/complaint line in place for the reporting and/or resolution of privacy concerns?

Uber Technologies was also included in RepRisk's Most Controversial Companies Report 2014 (page 7).

Case 3 Burger King criticized for alleged privacy violations of customers in Sweden

Company: Burger King
Country: Sweden

Sector: Travel and Leisure
Issue: Alleged spying on customers

RepRisk Incident: April 2015, originally reported in a Swedish-language source

Burger King's restaurant in Växjö, Sweden, has been criticized for secretly recording personal information about its clients through a camera-like device in its parking lot. The device has been in place for about one month and several clients have noticed its presence. However, the restaurant has allegedly not applied for permission to install a surveillance camera. The company in charge of the device is said to be Nordic Service Partners. A lawyer at the Swedish Data Protection Authority has warned that even if the camera does not violate legislation concerning surveillance equipment, the recording of clients' personal information through the photographing of their car registration plates, may fall under legislation pertaining to the storage of personal information. The lawyer claims that the manner in which the camera is operating will determine whether or not it is violating the privacy of Burger King's clients.

GEC Risk Analysis:

This is an example of an alleged personal data privacy violation in a country with a relatively strict data privacy legal regime and a consistent regulatory approach to investigation and enforcement of such laws. Reference to the Swedish Data Protection Authority and their statements seems to indicate that there is a proactive enforcement agency in charge of investigating and potentially prosecuting alleged violations.

The statements made by the agency's lawyer also suggest that the regulator may choose not only to enforce the law in clear-cut cases, but also in cases where the spirit of the law may have been violated. In other words, even though Burger King denies collecting or storing the private data of customers through their parking lot video camera, the mere fact that its recording devices pick up and store potentially private data of customers may lead to enforcement action by the agency against the fast food store even in the absence of a clear violation.

Key takeaways:

Some of the key takeaways and lessons from this case would include the following:

- In countries with more evolved privacy laws and regulators, businesses need to maintain a heightened awareness that laws may be interpreted more broadly. Actions that may be thought to be innocent may be subject to regulatory review and maybe even some form of enforcement action.

- Commercial establishments wherever located, but especially in jurisdictions with greater privacy law enforcement, should undertake a periodic assessment of how, what, and why they collect and store the private data of stakeholders including employees, management, customers, and third parties.

- Even in the absence of a clear privacy violation, the reputational risk consequences of not handling a data privacy situation to the satisfaction of key stakeholders could harm the short-term and even longer-term reputation of the particular company involved.

Case 4 US judge rules that Apple and 14 app developers should face data mining claims

Company: **Apple, Yelp, Electronic Arts, Twitter, Instagram, Rovio, and other app developers**
Sector: **Software and Computer Services**
Country: **United States of America**
Issue: **Corporate data mining**

RepRisk Incident March 2015, originally reported in an English-language source

A US District Court judge in California has ruled that Apple, Yelp, Electronic Arts, Twitter, Instagram, Rovio, and other app developers must face the majority of the claims in a class action lawsuit that accuses them of illegally collecting and sharing data from iPhones and iPads without the knowledge or consent of users. The original lawsuit was filed in 2012 against Path Incorporated, accusing it of collecting sensitive data about its users, including minors. The court ruled that Path had violated Federal Trade Commission rules by mining and storing data from minors, and Path agreed to strengthen its privacy policy. An amended lawsuit filed in Texas accused all defendants of invasion of privacy for using a "friend finder" feature on Apple's iPhone and iPad to gain information about the user's contacts. Although the judge dismissed most of the allegations due to lack of detail, he ruled that Apple will have to face claims related to the violation of California's false advertising, consumer, and unfair business practice laws. The plaintiffs accused Apple of knowing about its products' inherent defect, which allowed apps to access users' address book information, and of concealing the facts from consumers.

GEC Risk Analysis:

This fact pattern raises a major concern facing businesses and individuals in this age of hyper-transparency and super-connectivity: big data collection is everywhere, including unlikely places. Even generally law-abiding companies could struggle with the vast array of different privacy-related laws at the local, state, national, and international levels. If a company is doing business around the world, it has a gargantuan task to understand the number and complexity of overlapping and possibly contradictory privacy-related laws.

Because of the widely evolving legal and regulatory landscape regarding privacy, companies that are less scrupulous can potentially exploit inconsistencies and hide behind apparent loopholes. Thus, what might appear to be relatively innocuous "friending tools" may indeed be a devious way to get personal data, not only on the average adult, but also on the average child, for whom there are often additional legal protections.

In this particular case, there may be a mix of reasons why these companies have been the subject of lawsuits: Some of them may not have fully understood the implications of existing laws, while others may have taken full advantage of the possible loopholes.

Key takeaways:

There are a few protective steps companies and individuals should take in the face of the ongoing privacy confusion in the marketplace:

- Individuals should always read the terms and conditions when they purchase or subscribe to new software and other products and services.
- Companies need to develop internal checks and balances to ensure that they are abiding by applicable laws regarding privacy and data mining, especially those concerning the private data of minors.
- Companies should develop plain-language and easy to read and visible warnings for customers.
- Responsible companies should also develop a more comprehensive data and information security governance framework for their organization, and thereby create consistency in the application of responsible policies and legal compliance.

Case 5 Hitachi, NEC, and UBIC criticized over artificial intelligence software

Company: Hitachi, NEC, and UBIC
Sector: Technology Hardware and Equipment; Software and Computer Services
Country: Japan **Issue:** Monitoring of employees with artificiall intelligence

RepRisk Incident: February 2015, originally reported in an English-language source

The Electronic Privacy Information Center and other critics have expressed concerns over the use and development of artificial intelligence (AI) software in Japan, which can allegedly be used to spy on employees and thereby to compromise human rights and privacy. Companies including NEC, UBIC, and Hitachi have developed tools to gather data on employees' digital communications, such as emails and social media, in order to analyze and predict staff behavior. Companies, such as Mitsubishi and Mitsubishi Research Institute, have reportedly used one of UBIC's AI software products. Allegedly, this preventive profiling method can be programmed to flag anything deemed as inappropriate by the company.

GEC Risk Analysis:

This story illustrates yet another aspect of how data privacy can be eroded from a personal and professional perspective. In contrast to the many familiar technologies, such as the Internet, social media, and big data, we have not even begun to feel, let alone understand, the impact that artificial intelligence (AI) will have on our personal lives, work, the economy, business, government, and otherwise.

This story appears to involve the alleged use by Japanese companies of AI software that not only collects data on employees, but also uses this data to predict and interpret the behavior of employees. This purportedly allows an employer, in turn, to potentially make judgment calls or decisions about employees that could have negative consequences on their livelihoods, employment, or even reputation.

Such judgments could be reached even though the predicted behavior may not take place. Needless to say, the use of AI in the workplace in such a manner would raise a variety of legal, ethical, and fairness issues.

Key takeaways:

As "smart" big data or AI becomes more mainstream, the use and potential abuse of AI to predict not only personal but organizational behavior, actions, trends, and choices, will be on the rise. As these issues emerge, both people and organizations need to consider the following:

- The potential legal, regulatory, and reputational consequences for companies that use untested, uncharted AI tools in the workplace are very serious. Companies should move cautiously, understand the legal and ethical implications of these tools, and test any such uses very carefully.
- Organizations that misuse these tools could suffer the consequences not only from a legal standpoint but also the loss of reputation, and loss of the support and trust of stakeholders.
- Individuals who are on the receiving end of decisions occasioned by AI tools may not know that this is happening immediately, but as the reality and effects of AI-driven decisions become more common in the workplace, there will likely be more individual and collective demands for accountability from companies and others using these tools.

Case 6 Personal data of 80 million Anthem clients and employees hacked in system breach

Company: Anthem
Country: United States of America
Sector: Insurance
Issue: Hacking of patient information

RepRisk Incident: February 2015, originally reported in an English-language source

The health insurer Anthem, formerly known as WellPoint, has disclosed that hackers have stolen the personal information of approximately 80 million of its employees, as well as former and current clients. Reportedly, tens of millions of personal records including social security numbers, names, and addresses, have been exposed. The incident is under probe by the US Federal Bureau of Investigation and is considered to be one of the largest in the wake of similar hacking activities targeting other corporations recently. A cyber-attack on JPMorgan Chase allegedly exposed the data of roughly 76 million households (August 2014), while hackers who gained access into Home Depot's system reportedly compromised 56 million credit card accounts and 53 million customer email addresses (September 2014). Additionally, an infiltration into Target's system compromised the data of 40 million payment cards (December 2013). According to the Health Information Trust Alliance, the last known healthcare company data breach was the April to June 2014 cyber-attack into Community Health Systems, which affected the records of 4.5 million customers.

GEC Risk Analysis:

The hacking of healthcare companies and organizations is high on the agenda of both criminal enterprises and hackers working on behalf of foreign governments. The former are looking to use the information for other criminal commercial purposes, such as selling names, identification numbers, and addresses for a profit to other illegal or less than scrupulous enterprises.

Hackers are also aiming at longer-term, potentially more nefarious purposes. Some purposes are strictly commercial: by illegally collecting the intellectual property from other companies, they can help their own enterprises gain a commercial advantage. Or, in some cases, they may be looking to disrupt companies and their executives by using the personal healthcare data of key executives, for criminal purposes such as blackmail and extortion.

Ultimately, the illegal collection of healthcare data by hackers working on behalf of foreign governments can have even darker purposes, with wholesale biographical information, including data on family members, being built over time for purposes that are not even necessarily yet known even to the hackers themselves.

Key takeaways:

Healthcare organizations and financial institutions are among the sectors that need to have heightened vigilance regarding the protection of sensitive personal information. Healthcare organizations, including large health insurance companies like Anthem, have some of the most coveted and sensitive personal information of any organizations due to the nature of their business.

Companies need to spend time and resources devoted to finding solutions, building defenses, and proactively protecting their assets, as well as the assets of their customers and other stakeholders. Such defenses and protection should include:

- Understanding the company's vulnerabilities by conducting a cyber-risk assessment.
- Having a cyber-security risk and crisis team in place and ensuring that cyber-risk scenario planning and exercises are always part of the agenda.
- Having a cyber-governance program in place, including the CEO, C-Suite, and Board.

About RepRisk

RepRisk is a leading business intelligence provider specializing in dynamic environmental, social, and governance (ESG) risk analytics and metrics.

On a daily basis, RepRisk systematically screens big data from a broad range of open intelligence sources in 15 languages in order to identify, filter, analyze and quantify ESG risks (such as environmental degradation, human rights abuses and corruption) related to companies, projects, sectors, and countries. This external perspective provides valuable insight into whether a company's policies, processes and commitments are consistently translating into performance.

Since 2006, RepRisk has built and continues to grow the most comprehensive ESG risk database that serves as a due diligence tool and early warning system in risk management, compliance, investment management, corporate benchmarking and supplier risk. The database currently includes risk profiles for over 53,000 private and publicly-listed companies and 13,000 projects as well as for every sector, and country in the world.

Headquartered in Zurich, Switzerland, RepRisk serves clients worldwide including global banks, insurance companies, investment managers, and corporates, helping them to manage and mitigate ESG and reputational risks in day-to-day business.

RepRisk provides the transparency needed to enable better, more informed decisions. To learn more, please visit www.reprisk.com.

About GEC Risk Advisory

GEC Risk Advisory is a global governance, risk, integrity, reputation and crisis advisory firm providing strategic counsel and consulting services to boards, executives, investors and advisors, in multiple sectors including financial, utility, technology, manufacturing, infrastructure, think tank, higher learning and professional services.

Specialties include strategic and enterprise risk management; reputation risk & resilience workshops, risk-based crisis scenario planning, workshops and advice; architecture and alignment of governance, risk and reputation with business strategy; creating, evaluating and structuring global risk, ethics, corporate responsibility and compliance programs including global anti-corruption and supply chain; and Transforming Risk into Value workshops.

Our philosophy at GEC Risk is to provide our clients with a constructive, multi-cultural and strategic approach aimed not only at understanding and triangulating global risks but ultimately at improving stakeholder trust and enterprise value.

To learn more, please visit: www.gecrisk.com.

DISCLAIMER

The information contained in this joint report ("Report") is not intended to be relied upon as, or to be a substitute for, specific professional advice. No responsibility for loss occasioned to any persons and legal entities acting on or refraining from action as a result of any material in this publication can be accepted. With respect to any and all the information contained in this Report ("Information"), RepRisk and GEC Risk Advisory make no representation or warranty of any kind, either express or implied, with respect to the Information, the results to be obtained by the use thereof or any other matter. RepRisk merely collects information from public sources and GEC Risk Advisory provides generic, non-specific analysis of this data, which is distributed in the form of this Report.

RepRisk and GEC Risk Advisory expressly disclaim, and the buyer or reader waives, any and all implied warranties, including, without limitation, warranties of originality, accuracy, completeness, merchantability, fitness for a particular purpose and warranties related to possible violations of intellectual property rights, trademark rights or any other rights of any third party. This report may be quoted, used for business purposes and may be shared with third parties, provided www.reprisk.com and www.GECRisk.com are explicitly mentioned as the source.

METHODOLOGY

RepRisk Special Reports are compiled using information from the RepRisk database, which monitors environmental, social and governance (ESG) risks for companies, projects, sectors, and countries. The RepRisk database currently contains risk incidents on more than 53,000 private and publicly-listed companies. RepRisk analysts monitor the issues related to ESG risk across a broad shareholder and other stakeholder audience of NGOs, academics, media, politicians, regulators and communities. Once the risk incident has been identified with advanced search algorithms and analyzed for its novelty, relevance and severity, risk analysts enter an original summary into the database and link it to the companies and projects in question. No article is entered twice unless it has been escalated to a more influential source, contains a significant development, or has not appeared for the past 6 weeks.

All data is collected and processed through a strictly rule-based methodology. This helps to ensure the balanced and objective rating and weighting of the risk incident, and thus the company's quantitative measure of risk exposure, the RepRisk Index (RRI). The RRI measures the risk to a company's reputation, not its actual reputation.

REPRISK®
ESG Business Intelligence

GEC Risk Advisory
Transforming Risk into Value®

Contact Information

For more information about the RepRisk ESG Risk Platform or this Special Report, please contact **media@reprisk.com** or visit **www.reprisk.com**.

For more information about GEC Risk or its advisory services, please contact **abonimeblanc@gecrisk.com** or visit **www. GECRisk.com**.