Traversing the ethical and legal minefield associated with collecting and handling personal data

By Tiffany Stevens, President
CIBJO Ethics Commission
& Miya Owens, Associate Counsel, JVC

The last Ethics Commission Special Report, published in 2019, included a broad overview of the jewellery industry's ethical supply chain concerns, including manners of sourcing, human rights, accurate descriptions of products and fair advertising. The report, which can be downloaded and read by CLICKING HERE, emphasises that every player in the jewellery industry should address these topics in their core business practices.

The report concludes with a mention of the rapid evolution of technology, noting that "those who seek to deceive are able to create ever more complex products and manipulate data and information to achieve their aims."

Tiffany Stevens, President of the CIBJO Ethics Commission.

This is precisely what the commission will cover in this year's report, namely the legal and ethical implications of collecting and using personal data in the jewellery trade.

These concepts are vast and complex. But understanding the implications and incorporating robust data protection and cybersecurity practices into the culture of your businesses are essential to thriving in the current and future economy.

WHAT IS DATA AND HOW IS IT USED?

Before tackling this issue, there are a few basic concepts to review. The definition of the word "data" and the ways companies are harnessing and using data are both essential to understanding the vast issue at hand.

Data are facts or information used to analyse something. Personal data generally refers to information relating to a natural person (i.e., a human), whether this person is identified or unidentified. Examples of personal data include names, identification numbers, physical and digital addresses, and cultural identities.

Keep in mind that the different laws define "personal data" in different ways, so you should familiarise yourself with your country or state's relevant legal definitions and obligations related to personal and other data. Many businesses obtain personal data from customers and employees during in-person and digital interactions, such as conversations and interactions with websites and social media pages. Many businesses also utilize personal data obtained from third-party companies for analyses and operations.

Businesses across industries have successfully been harnessing data for years. Retailers using clusters of internal and external data are now able to quickly develop comprehensive, personalized promotions for their consumers. Businesses using data from cookies are now able to gain valuable insights into their website visitors' behaviors, such as which pages are visited the most, the time spent on certain pages, and how visitors found the website. Cookies are also used to automate targeted advertising and more. Businesses are using artificial intelligence (AI) to streamline their hiring processes and provide website users with tailored product recommendations and retail experiences. The possibilities of data use are vast and everchanging.

To survive the COVID-19 pandemic, businesses have had to increase the agility of their operations to keep up with changing consumer behaviors and purchasing patterns, making data harnessing and analysis more relevant and necessary than ever.

According to a *Harvard Business Review* article, organisations with data-driven operations can outperform their peers by an average of 5 percent in productivity and 6 percent in profitability[1]. That said, with an increased reliance on data for business operations, jewellery businesses of all sizes should be aware of the legal and ethical implications of data use.

THE DATA PROTECTION LEGAL LANDSCAPE

With the proliferation of data collection and use in our technology-driven society, there is a concurrent increase

1. Andrew McAfee, Erik Brynjolfsson, "Big Data: The Management Revolution,"Harvard Business Review, October 2012, https://hbr.org/10/2012/big-data-the-management-revolution.

Co-author, Miya Owens, Associate Counsel, Jewelers Vigilance Committee (JVC).

in laws and regulations worldwide promulgated to address the inevitable corresponding legal risks. These laws and regulations often have a few common goals: to increase organisational transparency related to data collection and usage, to increase consumer rights related to their data, to increase an organisations' obligations in protecting data and to decrease the likelihood of personal data falling into the hands of bad actors or uses without consent. With these overarching goals in mind, every business has an obligation to its consumers and employees to collect and use data compliantly and ethically.

While the legal landscape related to data use and protection is rapidly changing, all businesses should be cognisant of the relevant laws and regulations in all jurisdictions where they have physical and digital ties. Gone are the days of only complying with the laws of jurisdictions where a business has a physical presence.

Most, if not all, data-related laws are applicable to businesses that simply allow users or "data subjects" (as natural persons are often called under the law) to browse their websites and therefore interact with the site's cookies and other data tracking technologies, even if the data subjects don't purchase any goods or services. In the past decade, data security laws and regulations have continued to place increasingly stricter obligations on businesses across the world and enforcement bodies are imposing costly penalties on businesses who fail to comply with these obligations.

For example, the EU's General Data Protection Regulation (GDPR) set the legal landscape ablaze when it was passed by the European Parliament in 2016, giving applicable businesses about two years to prepare for its effective May 2018 date. The GDPR, which still stands as the toughest privacy and data security law in the world, applies extraterritorially, meaning it may apply to a business located outside of the EU, so long as it offers goods or service to EU customers or monitors the behavior of EU-based website visitors through web tools such as tracking cookies[2].

Among other things, the GDPR requires organisations to implement data protection "by design and default," meaning data protection principles should be considered during the design of every project and activity your organisation undertakes. The GDPR also provides EU data subjects with certain rights, which relevant organizations must honour, including the right to be informed of data collected, the right to access data collected, the right to erasure and more[3].

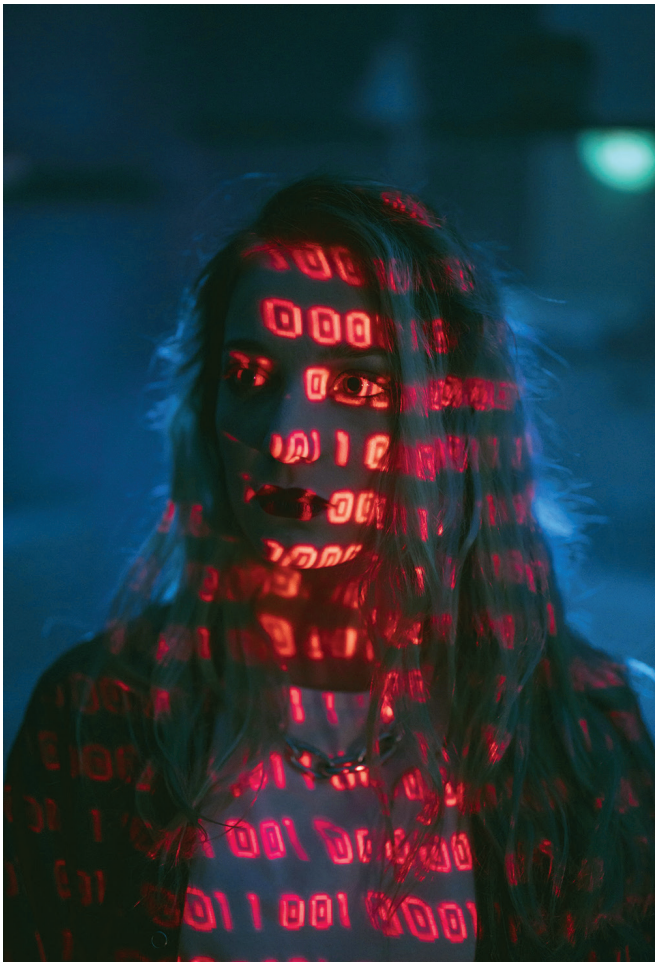
The GDPR also requires organisations to implement appropriate technical and organizational measures to ensure that the requirements of the GDPR are met and data is protected, which could involve two-factor-authentication for employees to access personal data, encryption of data, company-wide trainings and limiting access to the personal data of your customers and employees.

This law also requires organisations to obtain consent from data subjects prior to processing data. Notably, the GDPR also requires organisations to document whether personal data is being processed for a legitimate interest and limit processing accordingly[4].

2. Horizon 2020 Framework Programme, "Does the GDPR apply to companies outside the EU?," https://gdpr.eu/companies-outside-of-europe/.

3. Horizon 2020 Framework Programme, "What is GDPR, Europe's new data protection law?," https://gdpr.eu/what-is-gdpr/.

4. See footnote 3.



What constitutes a legitimate interest requires a thorough review of the law and an organisation's business functions. Similar reviews are required for compliance with Brazilian and Canadian legislation, and the new and revised data protection laws of other countries.

In the United States, there is no omnibus federal privacy law, but rather a network of federal laws that cover specific types of data such as health data, education records and video rental records, and, of course, an ever-growing collection of state privacy and data protection laws.

California's Consumer Privacy Act (CCPA)[5], dubbed by many a "mini GDPR," passed in 2018 and became effective on January 1, 2020[6]. This law, the United States' first comprehensive privacy law, provides California residents with new privacy rights, including the right to know about the personal information a business collects about them and how it is used and shared, the right to delete personal information collected, the right to opt-out of the sale of their personal information and the right to non-discrimination for exercising their CCPA rights[7].

Similar to the GDPR, the CCPA applies extraterritorially, but its scope is limited to for-profit businesses that meet at least one of the law's three prongs: 1) have a gross annual revenue of over $25 million; 2) buy, receive or sell the personal information of 50,000 or more California residents, households, or devices; or 3) derive 50 percent or more of their annual revenue from selling California residents' personal information[8].

Applicable businesses must now give consumers certain notices explaining their privacy practices and respond to California resident inquiries and requests, among other obligations. In November 2020, the CPRA, a ballot initiative to amend the CCPA, was passed by California voters. Most of the CPRA amendments will become fully effective on January 1, 2023.

Following California's lead, additional states including Virginia and Colorado have also enacted comprehensive privacy and data protection laws.

LEGAL AND ETHICAL IMPLICATIONS FOR JEWELLERY

An Internet search of "data breach" will elicit thousands of examples of businesses who failed to implement data protection principles in their businesses, exposing the sensitive personal and financial information of their customers and employees, and exposing the businesses to harsh legal penalties and reputational harm.

The Internet also reveals just as many examples of companies that have either failed to inform or have blatantly deceived consumers about their data collection, use and sharing practices. For example, this past July, the Luxembourg data protection commission conducted an investigation of Amazon Inc. and later issued the retailer a 746 million euro fine. The commission's fine, which Amazon is disputing, relates to Amazon's use of consumer data in targeted advertising[9].

As another example, in 2017, the credit reporting agency Equifax announced a data breach that exposed the personal and financial information of nearly 150 million people. This breach was reportedly the result of the company's failure to update certain databases and resulted in a settlement

5. To view the text of the law, visit https://leginfo.legislature.ca.gov/faces/codes_displayText.xhtml?division=3.&part=4.&lawCode=CIV&title=1.81.5

6. In November 2020, the CPRA, a ballot initiative to amend the CCPA was passed by California voters. Most of the CPRA amendments will become fully effective on January 2023. See, e.g., https://iapp.org/resources/article/california-consumer-privacy-act-of2018-/.

7. California Attorney General CCPA Overview, https://oag.ca.gov/privacy/ccpa.

8. See previous footnote.

9. Stephanie Bodoni, "Amazon Gets Record $ 888 Million EU Fine Over Data Violations," Bloomberg, July 2020, https://www.bloomberg.com/news/articles/30-07-2021/amazon-given-record-888-million-eu-fine-for-data-privacy-breach.

payment of over $400 million to help people affected by the breach[10].

A lesser-known ethical issue involving the use of data is artificial intelligence's exacerbation of racial and gender bias. In the same way companies like Netflix use AI to tailor show and movie recommendations to subscribers, many retailers are now using AI to offer their customers personalized retail experiences[11].

Companies across industries are also using AI to streamline their hiring practices. But, because AI is based on data from human decisions, the prejudices and biases present in their rationale has made its way to the computer-based AI decisions. One example of this was Amazon's AI-based hiring tool that was discovered in 2015 to favor men for technical jobs because the tool was trained to sort applicants based on patterns in resumes submitted to the company, the bulk of which were from men[12].

Based on this discovery, Amazon ditched the tool. Read about several other AI bias examples here: https://towardsdatascience.com/real-life-examples-of-discriminating-artificial-intelligence-cae395a90070.

Hopefully the above examples encourage all readers of this report to seriously consider the implications of data use in their businesses and proceed with caution and an eye towards compliance and consumer protection.

DIRECTIVES FOR JEWELLERY BUSINESSES

The Ethics Commission offers the following directives aimed at minimizing the dangers of misusing or mishandling customer and employee personal data.

1. **Conduct a thorough analysis of the data you, your business partners, and third-party companies collect, use and share to assess your legal and ethical data use obligations.**

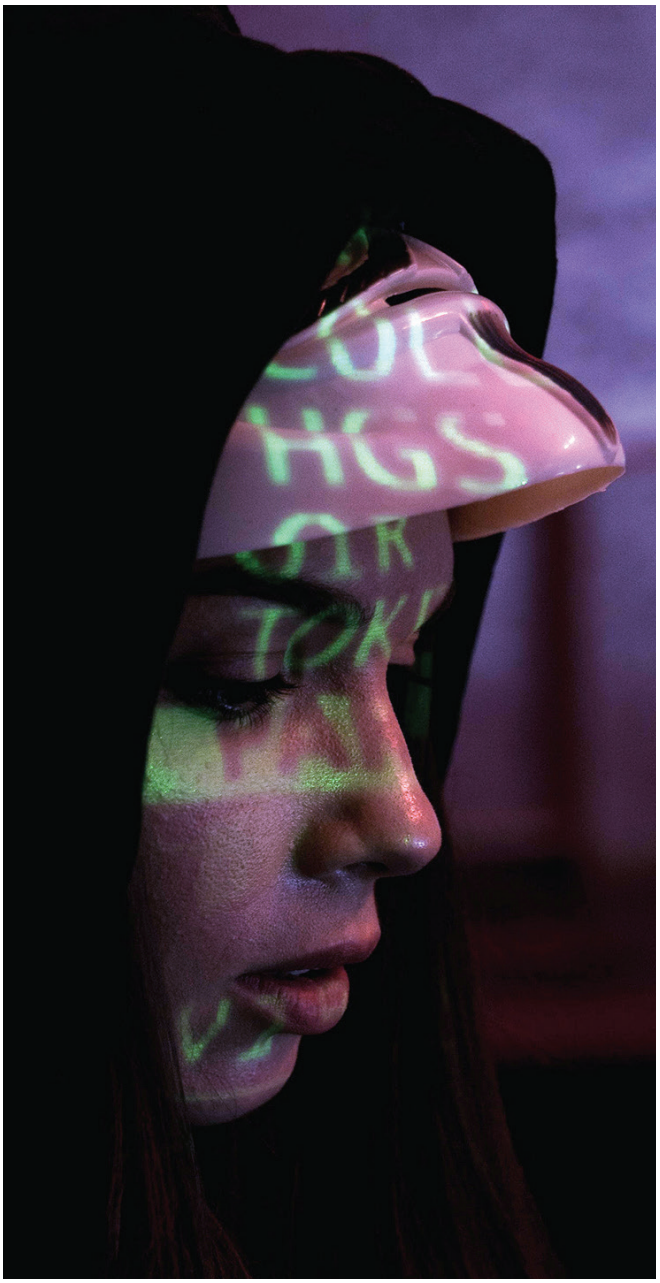
Ask yourself the following questions: Where are your "data subjects" located and do these locations require your business to comply with data protection laws? What kinds of data are you collecting and why?

With an increasing pressure to minimise the data collected and used by businesses, you want to ensure that you, your business partners and third-parties you engage with (such as analytics companies) are not collecting, storing, selling, sharing or misusing data.

You also want to minimise the amount of data that you collect, use and share. Only collect the data you actually need for your business to function and ensure that your company properly discloses this collection and use to your data subjects.

You also want to ensure that you, your business partners and third-parties are not using data to discriminate against customers or employees. Your data practices should always align with your legal obligations and disclosures made to consumers.

10. Federal Trade Commission, "Equifax Data Breach Settlement," January 2020, https://www.ftc.gov/enforcement/cases-proceedings/refunds/equifax-data-breach-settlement.
11. See Ingo Willems, "The future of e-commerce is being massively influenced by the use of artificial intelligence,"… June 2020, https://dmexco.com/stories/using-ai-to-create-a-personalized-shopping-experience-in-online-retail/.
12. The Guardian, "Amazon ditched AI recruiting tool that favored men for technical jobs," https://www.theguardian.com/technology/2018/oct/10/amazon-hiring-ai-gender-bias-recruiting-engine.



2. Draft and revise transparent privacy policies and procedures and ensure they are operationalised and considered in every business decision.

Not only is this directive required by most data protection laws, but consumers are demanding that businesses are transparent about data collection and use, and they expect all businesses to protect their personal data.

Your policies should not only disclose the types of data you are collecting, using, and sharing but should also disclose the reason for each collection and use.

Whether or not you are required by law to provide data subjects with an opt-out function or other rights, you may want to consider providing this function and other rights to consumers to enhance their trust in your business.

And, as with any policies and procedures in your businesses, you need to regularly revisit and fine tune these documents and ensure they are operationalised and effectively protecting personal consumer and employee data. Protecting personal data should be a company imperative and should be considered in every decision your organisation makes.

3. Limit the accessibility of data by implementing the best cyber-hygiene practices in your businesses.

These practices include limiting access to data to only those in your organisation who need it and protecting digital and physical data with multi-factor authentication, strong passwords, secure locks, encryption and more.

All hardware and software programs used in your businesses (including personal devices) should be kept up-to-date, as updates often contain security patches that will minimise the likelihood of exposing personal data.

Consider hiring professionals who can assist your business in implementing the best cyber-hygiene practices.

4. Ensure that your third-party vendors are up to par with their data protection infrastructure.

Many data breaches have a root case in third-party vendors, so verify that your vendors have a data protection infrastructure that is equal to or better than your business's infrastructure.

5. Consider cyber insurance and counsel for your businesses.

Even companies with robust data protection policies and procedures are at risk for breaches and data misuses, both of which can be financially and reputationally costly. Many existing and new insurance companies now offer policies that will allow businesses to offset the costs of breaches and cyber-attacks.

Conclusion

Every member of the trade, regardless of size, location and business type, should be emphasising the importance of data protection from the legal compliance and ethical perspectives, as the two perspectives are inextricably intertwined in today's digital world.

If you follow the above directives, hire the appropriate experts, and consider the legal and ethical implications of data use in all of your organisation's decisions, you can successfully use data to improve your business while also maintaining your reputation and minimising potential harm to consumers and employees.

CIBJO CONGRESS 2021

Like many industry events held since the COVID-19 pandemic began, the 2021 CIBJO Congress is taking place virtually.

The Ethics Commission is conducting two online sessions and the congress, in the form of webinars organized together with the Marketing and Education Commission, which is a headed by my colleague, Jonathan Kendall.

The first webinar already took place on November 15, 2021. It focused on subjects related to social and environmental responsibility. Participating was a new CIBJO Committee that is currently developing a set of harmonised terminology relating to responsible supply chains in the industry.

The second webinar will be on Thursday, November 18, 2021, at 3:00 PM Central European Time, or 9:00 AM U.S. Eastern Time. It will concentrate on the impact of new technologies, particularly where they are related to the marketing of jewellery in the retail environment, and focus on issues raised in this Special Report, which is the collection and use of personal data to better serve the consumer, while still complying with international privacy and data use laws.

Co-presenting the webinar on November 18 will be CIBJO's new Technology Committee. A registration link is available by CLICKING HERE.

Updated information about the congress can be viewed online at: http://www.cibjo.org/congress2021/.

PHOTO CREDITS

Cover photo, page 3 photo and page 4 photo by Cottonbro on Pixabay.com

Page 5 photo by Mati Mango on Pixabay.com

Page 6 photo byTima Miroshnichenko on Pixabay.com