Data Regulation Implications for Robo-Advisory

Alexander Helter, CFA, FRM, CAIA

Management Consultant, Stradegi Consulting

stradegi

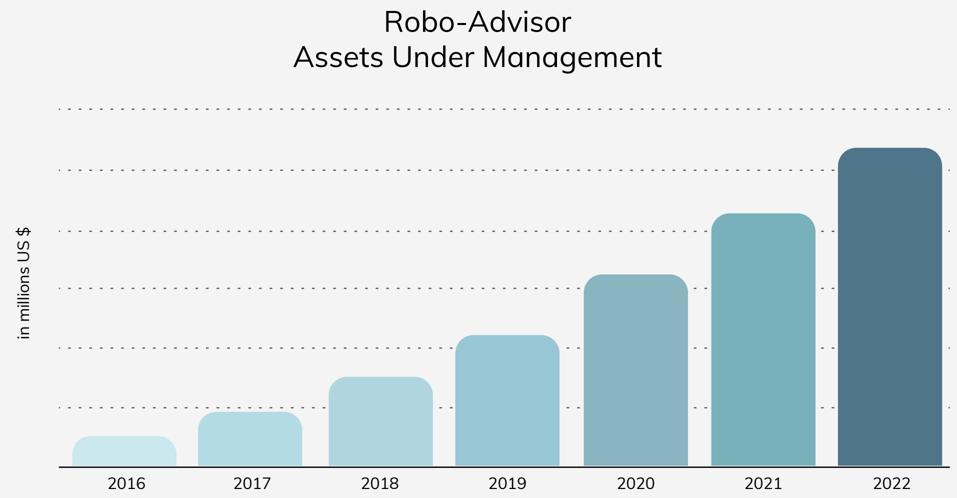
August 2019

Introduction

In this paper, Alexander Helter summarizes some of the thoughts he presented at both the 2018 Singapore Management University Sim Kee Boon Institute for Financial Economics Conference “Charting a Roadmap towards a New Data Regime for the Digital Economy” and the Asia-Pacific Economic Cooperation Policy Support Unit task force “Fostering an Enabling Policy and Regulatory Environment in APEC for Data-Utilizing Businesses”. Elements from this paper and his speech were incorporated into the Asia-Pacific Economic Cooperative Finance Ministers’ “Roadmap for New Financial Services Data Ecosystem”. As data privacy and governance takes a global focus with the advent of GDPR, “robo-advisors” are in the spotlight for review. Investors have embraced these robo-advisors as a platform for more efficient and lower cost investing. This has caused increased interest from global regulators to better understand the data and algorithms used to drive the robo models, in order to protect consumers and the financial markets.

Robo-Advisory’s growth & concerns

The robo-advisory business is growing at a rapid pace, and it doesn’t show signs of stopping anytime soon. AUM at robo-advisors has grown nearly 300% in the last 2 years to US$371B as of May 2018 (Statista 2018), and robo-advisory is projected to be utilized in some form for 10% of global AUM within 3 years (MyPrivateBanking 2017), $500B of which alone could be in APAC (Araneta, Agrawal and Kapoor 2017). While all this growth in an innovative area of finance may have positive implications, one of the areas coming into the limelight is the regulation of the data driving the technology.


Robo-Advisor
Assets Under Management

Source: Statistics, May 2018: Selected region may include countries listed in Digital Market Outlook

Robo-advisory requires immense amounts of big data; data which also includes personal data to assess things, such as client demographics, risk tolerances, and wealth levels. Recent data breaches across all industries have cast doubt that user data is truly secure. Even financial institutions, which as an industry were thought to have some of the most robust cyber security systems infrastructure in place, have seen massive breaches last year, including breaches at the US credit agency Equifax breach (Federal Trade Commission n.d.) and the Italian bank UniCredit SpA (Arnold 2017). These events, combined with the advent of the enforcement date of the EU's GDPR, or General Data Protection Regulation legislation, are causing many regulators to re-evaluate the data governance policies in place that will help protect user privacy. Given their emerging and fast-growing nature, it is no surprise that financial regulators such as FINRA have their data governance sights locked on to robo-advisors.

The source of Robo-Advisory growth

Automated financial planning and portfolio management software, commonly referred to as "Robo-Advisors" are a relatively new entrant into the financial markets. Using computer algorithms to automate much of the traditional portfolio construction process, robo-advisors seek to displace human advisors in favor of machine processing to perform asset allocation and rebalancing activities for investors. There are many robo-advisors operating in the market trying various differentiation strategies, however the general selling point for why consumers should choose a robo over a human is the lower fees that come with passive and computer-based investment strategies, coupled with the technology interface.

Many larger financial institutions are aware of the strong selling point of lower fees. While there are some completely independent robo-advisors, many are either subsidiaries of, or have strong business connections to, established investment firms. Established investment firms see robo-advisory businesses as a means to attract a specific segment of the investor market, namely those clients with either not enough investment wealth to make a human-advisor relationship financially feasible, or clients who desire a lower-cost alternative. An established firm can offer their robo-advisory product to younger clients with limited or no investment wealth, as many robo-advisories offer accounts with minimums as low as $50. Once they have helped that client save diligently through monthly investments, the portfolio may become large enough to meet the established firm's normal brokerage account minimums of generally $2,000 or more. This means that low expense robo-advisory products at these established firms can serve as an incredibly effective tool. The low minimums can help investors bridge the gap between having no savings, the generally large minimums necessary to do self-directed investing, and the even higher minimums necessary for a managed account or traditional financial planning.

However, as relatively new ventures, there is not a comprehensive understanding of the type of data robo-advisors may need to collect, how that data may differ from traditional financial institutions, and the appropriate protocols to handle that data, which generally includes information and interaction from the user's smartphone.

The need for GDPR and Data Privacy Protections

GDPR is a substantial revision to the prior European data privacy policy DPD, the Data Protection Directive, that for the most part was developed before the internet was considered mainstream. When DPD was drafted, some of the best practices for data handling at the time included policies on the alphabetical ordering of paper HR filing systems – something that today would seem quite antiquated. 20 years ago, regulators couldn't have foreseen the potential that someone could have records on an individual's entire purchasing history through Amazon and other merchants, travel and lifestyle behavior through Facebook and other social media, web history through Google, dating activities through Ashley Madison, biometrics through Aadhaar, and other personal information. Nor could they foresee the ease with which an unscrupulous criminal could steal the personal records of not just a handful of people but rather hundreds of millions of individuals with only a single breach.

The emerging technology utilizing the internet and IoT, Internet-of-Things, devices aimed at capturing big data has reshaped how data regulators need to evaluate data privacy and governance. While GDPR addresses many principles-based best practices on data governance and privacy protection, two of the areas it is most widely known for are the substantial increase in penalties for a firm neglecting its duties as a steward of "PII", Personally Identifiable Information, and the obligation to alert the respective regulatory authorities within 72-hours of discovery of a data breach. (Publications Office of the European Union 2016). The theme being expressed by EU regulators is that firms need to better understand the data they collect, understand their role as a steward of users' data charged with its proper protection, and bear the responsibilities if that data is lost or misused like any other valuable asset, including proper notification and potential financial consequences.

Regulators Focus on Global Best Practices

While GDPR is Europe's attempt at a framework for data governance policies that better address recent technological advancements, corporations would be remiss to think GDPR only impacts Europeans. While the policies themselves are only set to regulate European companies, or companies who intentionally target the collection or processing of data on European residents, the expected impacts are more

Principal, Data Synergies Pty L
ABAC
APEC Business Advisory Council
IFC
International Finance Corporation
WORLD BANK GROUP
SMU
SINGAPORE MANAGEMENT UNIVERSITY

widespread. Already firms in the US and APAC are evaluating whether their company will be subject to GDPR based on their business dealings. Additionally, regulators have been evaluating GDPR as a framework for their own regional policies or updates to existing policies. As Singapore regulators noted in their PDPA, Personal Data Protection Act of 2012, “In the development of this law, references were made to the data protection regimes of…the EU, UK…and takes into account international best practices on data protection.” (Personal Data Protection Commission 2018) Newly implemented data protection policies in China, namely GB/T 35273-2017, also address handling of personal data. (Standardization Administration of the People's Republic of China 2017)

Although regulation policies in the US and APAC differ from GDPR, they maintain similar themes. EU and other global regulators seem to be focusing on principles-based standards, with a focus on user consent, data controller responsibilities, and data retention policies. Regulators are increasingly collaborating to standardize and develop common frameworks for cross-border policy, and data protection is no different. Even if a firm believes GDPR does not apply to their business practices currently, it is no excuse for a firm to disregard the policies. Corporations should expect that similar principles on data protection espoused under GDPR, and the corresponding penalties for failing to properly protect this data, will likely be implemented in local regulations in the near future as regulators continually update to global best practices

The new PII that Robos could expose

A special nuance of data privacy at robo-advisors that is not typically present at traditional financial service institutions is the information that the investment portfolio itself may disclose. Many robo-advisors attempt to appeal to younger millennials by aligning their personal values with their investment values. Motif Investing, a US-based robo-advisor operates a platform that encourages users to invest in thematic portfolios, or “Motifs”, set to profit from specific trends. (Motif Investing 2018) Clients select certain Motifs, portfolios of roughly 5-30 securities, and allocate their money into those Motifs. While this has its appeals, it also has potential data privacy risks. How professionally damaging might it be if, for example, a prominent environmentalist was found to have a sizable portion of their investment portfolio set to specifically profit from fracking or shale oil? What might a congressperson’s constituents say if their political rhetoric advocated for the repeal of Obamacare, but their investment portfolio was set to specifically profit from its continued existence? Or if pundits took to TV interviews denouncing gun violence, but invested in a portfolio containing only weapons manufacturers? Each of these are specific portfolio themes offered by Motif Investing.

An individual may decline to state publicly what their political affiliation is, but if a data breach at Motif revealed that the same individual had allocated some of their investment portfolio towards a Motif titled “Republican Donors” which is set to profit by “Counting on the GOP to Move Ahead” (Motif Investing 2018), their political affiliation may seem quite obvious. While Motif hasn’t sustained a known data breach, it is clear that the type of information a robo-advisor has on an individual could be much more in-depth and revealing than the type of data that could be gleaned from other financial institution data breaches, such as the 2014 JP Morgan data breach.

Data Governance Practices that Robos can employ

Robo-advisors generally employ the same data security and governance infrastructure that other larger financial firms do, however robo-advisors are arguably more data-driven. Robo-advisory heavily relies on big data and algorithms to perform many of the functions a human typically would – some functions to a purely automated level. This requires heightened security on the protection of those data pipelines and algorithms to prevent against intrusion, to avoid breaks in the data chain or modification to the algorithms that could cause inadvertent allocation behavior. The potential for significant data breaches at robo-advisors makes it all the more important that data storage best practices are employed.

Robo-advisors generally employ the same data security and governance infrastructure that other larger financial firms do, however robo-advisors are arguably more data-driven. Robo-advisory heavily relies on big data and algorithms to perform many of the functions a human typically would – some functions to a purely automated level. This requires heightened security on the protection of those data pipelines and algorithms to prevent against intrusion, to avoid breaks in the data chain or modification to the algorithms that could cause inadvertent allocation behavior. The potential for significant data breaches at robo-advisors makes it all the more important that data storage best practices are employed.

Three of the most relevant best practices for robo-advisors, and good practices advocated by GDPR and the data security profession, include pseudonymization of PII data, firewalls for any connected servers, and applying the principle of least privilege. Pseudonymization is the process by which a pseudo name, or code name, is created and associated for each real user. Data records can then be stored with pseudo names instead of the real names. With a pseudo name to real name key being kept on a different server, if a hacker could gain access to the pseudonymized data records on one server, but not the key kept on a different server, the data privacy of the users would still be intact. Ensuring that the networked servers are properly firewalled further assists in protecting against external threats from hackers. Finally, by ensuring that internal users only have as much access to various system privileges and data as are necessary for their job role, robo-advisors applying the principle of least privilege protect against data access if a hacker can gain access to the system. By combining all three best practices, robo-advisors can help ensure that even if hackers can penetrate their systems and access secured data stores, the resulting data breach may not provide data that can be directly linked to the specific users.

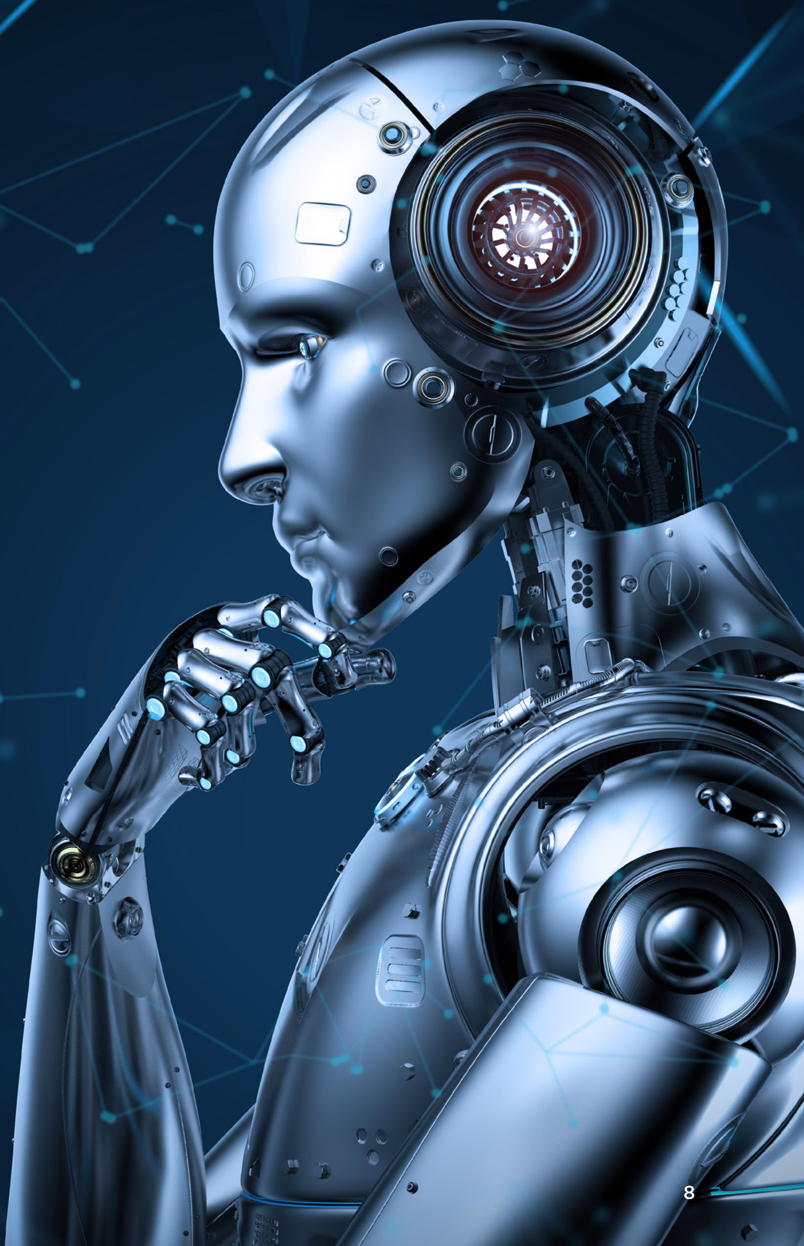
The weakest link may not be Robos, but Users

While financial institutions generally take network security and data protection seriously, end users don't always bring the same level of caution. User interaction with robo-advisors predominately occurs via smartphones or a web browser. While this provides ease of accessibility for the user, it also places a heightened burden to protect account security and data on the user. Leaving a smartphone unlocked, using weak passwords or storing them in a web browser, and other poor security practices by users could compromise the user's account in ways that the robo-advisor would have trouble protecting against. Users can help protect their own data by using strong passwords and employing other good practices such as enabling 2FA/MFA, Two-Factor or Multi-Factor Authentication, where account access requires not only knowing the correct password but also possessing a device such as an OTP from the user's phone or hard token. Users should also be aware of the software and apps that they install onto their computers and mobile devices, to ensure there isn't malicious code that exposes a backdoor for hackers to gain easy access to the data on the device. Hackers will generally look for the weakest point of entry, so users should make sure they are playing an active role in keeping their data secure and not allow themselves to be that weak link.

Regulatory solutions to Robos

Robo-advisors and robo clients will each undertake their own efforts to protect themselves, but regulators have a role to play as well. As noted before, robo-advisors are centered around algorithms that use big data to arrive at ideal allocation models for investors. Tom Baker and Benedict Dellaert of the Penn Wharton Public Policy Initiative have suggested that, to protect the investing public, regulators should be focusing on transparency and validation of those algorithms to ensure they are well understood and well tested. (Baker and Dellaert 2017)

Asset allocation algorithm models rely on expected risk, return, and correlation data of various asset classes to determine the optimal mix of these assets for any investor. These estimates are usually based on a combination of historical observations and forward expectations. However, some asset classes like US Equities have decades of daily return history, with clear and verifiable price transparency. Other asset classes, such as infrastructure investment funds, may only have a few years of monthly returns history, with lagged pricing and lower transparency due to fewer and more private deal transactions. These differences in return series can make it difficult to ensure expected risks and returns are evaluated over similar business cycles, and that the correlation between these assets are well understood when there are potentially very few data points.



Because of this, regulators should be looking into how the data being used in robo-advisor algorithms is being sourced, and how the models are handling gaps or potentially erroneous data, especially if the regulator has the authority to improve the capital market data quality through its regulatory power in the markets.

Robo-advisor asset allocation algorithms try to optimize portfolios based on generic asset classes, but after the model determines the weights, investors have to invest in actual financial products, such as Exchange-Traded Funds (ETFs). Although there is disagreement on identifying the best-in-class products for each asset class, independent investors would usually evaluate the quality of products based on low management fees, high market liquidity, and low tracking error to the benchmark. Robo-advisors generally already determine which products their clients will invest in, so users would be wise to understand how that selection was made. Ideally the robo-advisor would also be objective in determining which product or family of products to use for their models.

However, as noted, there are a number of robo-advisors that are either subsidiaries of, or otherwise backed by, larger financial firms. There may be an inherent preference to use an in-house financial product of their parent or partner financial firm, rather than evaluating investment options based on more objective criteria. There is nothing inherently wrong about this, but regulators should ensure robo-advisors are transparent in the explanation of why certain financial products were selected for use by the robo-advisor. This way, users can understand the driving forces behind the financial products that the robo-advisor is recommending for investment.

It is only after the algorithms have run and the portfolio is built that the quality of the model can be backtested. The aim of robo-advisors is to replace the need for humans to perform similar job functions, namely the portfolio optimization process from known capital market inputs and the evaluation process of the objectives and risk tolerances of their clients to determine an appropriate risk level for the portfolio. Therefore, the test of whether robo-advisors are working as intended is to check their output models and determine if a qualified financial professional would have come up with a similar looking portfolio based on the same inputs. The US Financial Industry Regulatory Authority (FINRA) noted in a Digital Investment Advice report just how important this verification can be. (The Financial Industry Regulatory Authority 2016) In a consultant study across multiple robo-advisors, the same client inputs for an example 27-year old man resulted in widely different asset allocations. These allocations varied by nearly 40% for their Equity allocation amounts, showing that the driving algorithms of robo-advisors can be very different between firms.

This highlights the importance for applying a prudent person check on the recommended portfolios that robo-advisor algorithms generate, to ensure that the computer is behaving reliably and constructing portfolios that are consistent with what a qualified financial professional would have built.

Future Outlook

Innovations in finance can help benefit the market, through increasing access to services that were previously unobtainable or too expensive for consumers. However, with those increased benefits come enhanced responsibilities to react to the emerging technology and ensure it isn't abused. Robo-advisors can help less affluent investors start saving, or push investors into properly diversified portfolios instead of concentrated stock positions. But they add a new layer of data protection concerns that regulators must be prepared to address. By collaborating with other global agencies, regulators can focus on transparency of both the driving algorithms and the business model of the robo-advisor to help protect the investing public from the downside of AI-driven investing. As for protecting user data privacy, best practices such as pseudonymization, limiting access, and firewalls prevail as good practices in robo-advising, as they do for other financial service firms. Users should also ensure they are protecting their data as well through good physical security, and using strong passwords combined with Multi-Factor Authentication. As the segment matures, robo-advisors should expect to see regulators increase the amount of oversight they exert to protect public interests and avoid potential data breaches or model risk from the algorithms.

References

Araneta, Michael, Anuj Agrawal, and Sneha Kapoor. 2017. Robo-Advisory: Changing the Face of Wealth in Asia/Pacific. October. Accessed June 05, 2018.

https://www.idc.com/getdoc.jsp?containerId=AP43074317.

Arnold, Martin. 2017. UniCredit reveals data breach affecting 400,000 customers. July 26. Accessed June 05, 2018. https://www.ft.com/content/229f89d2-71e6-11e7-93ff-99f383b09ff9.

Baker, Tom, and Benedict Dellaert. 2017. Regulating Robo Advisors: Old Policy Goals, New Challenges. Issue Briefs, Philadelphia, PA: Penn Wharton.

Federal Trade Commission. n.d. The Equifax Data Breach. Accessed June 05, 2018.

https://www.ftc.gov/equifax-data-breach.

Motif Investing. 2018. Republican Donors. Accessed June 05, 2018.

https://www.motifinvesting.com/motifs/republican-donors.

—. 2018. Why Thematic. Accessed June 05, 2018. https://www.motifinvesting.com/why-thematic.

MyPrivateBanking. 2017. Robo Advisors vs. Human Financial Advisors: Why Not Both? November 21. Accessed June 05, 2018.

http://www.businessinsider.com/hybrid-robo-advisors-will-manage-10-of-all-investable-assets-by-2025-2017-11-21/?IR=T.

Personal Data Protection Commission. 2018. Personal Data Protction Act Overview. February 21. Accessed June 05, 2018.

https://www.pdpc.gov.sg/Legislation-and-Guidelines/Personal-Data-Protection-Act-Overview.

Publications Office of the European Union. 2016. "L 119." Official Journal of the European Union 1-88.

Standardization Administration of the People's Republic of China. 2017. GB/T 35273-2017. December 29. Accessed June 05, 2018.

http://www.sac.gov.cn/was5/web/search?channelid=97779&templet=gjcxjg_detail.jsp&searchword=STANDARD_CODE=%27GB/T%2035273-2017%27.

Statista. 2018. Digital Market Outlook. Market Outlook, New York City: Statista.

The Financial Industry Regulatory Authority. 2016. Report on Digital Investment Advice. Regulatory Report, Washington D.C.: FINRA.