The ethical challenge of using healthcare data for patients with mental health issues

S3892026 | Data Driven Policy Making 2024 | Final Paper

Introduction

This article focuses on the ethical challenge of using healthcare data for patients with mental health issues. This topic is closely related to the question, "How does big data analytics challenge policymaking processes?" in the following ways:

1. Public health policymaking is increasingly driven by big data(*The Rise of Digital Health Technologies During the Pandemic | Think Tank | European Parliament*, n.d.), especially during the pandemic when many governments established online health management systems for their populations. In the field of mental health, big data analytics can help governments create more precise and effective public health policies.

2. The growing importance of mental health has gained more attention from policymakers. However, data related to mental health patients often includes highly sensitive information(Watson et al., 2023), such as personal details, emotional states, and experiences of trauma, which are more private than general medical data (e.g., blood pressure). Additionally, mental health issues are still stigmatized in many societies(*Stigma, Prejudice and Discrimination Against People With Mental Illness*, n.d.). If such sensitive data were to be leaked during the policymaking process, it could have severe negative impacts on patients' personal and professional lives.

This essay uses the example of Finland's 2020 Vastaamo data breach (a hacker stole sensitive client information from a government-collaborated psychotherapy center, and used it for blackmail; it was one of the most severe data breach case in Finland, even within Europe). With the help of principal-agent theory, the essay analyzes how the case can be interpreted using this framework: first, it reviews the development of the theory; next, it introduces the Vastaamo case, and examines how it supports the theory in some aspects and challenges it in others; finally, it proposes potential technical solutions in order to try solving the most critical issues stressed by this case.

Theoretical Foundation

The theory used in this essay is the principal-agent theory, which was first introduced in the field of corporate management by Jensen and Meckling*(Jensen & Meckling, 1976)*. They argued that separating ownership and control in a company can lead to principal-agent problems. Later, Moe(1984) expanded on this theory in the context of politics and public policy in his paper *The New Economics of Organization*. Moe explained that, in the political domain, the principal is usually the policymaker, such as government officials, legislative bodies, or even the public. The agent is the institution or individual responsible for implementing the policy, such as bureaucracies, private contractors, or technology firms(Moe, 1984).

The principal-agent relationship often faces three challenges(Moe, 1984):

1. Information asymmetry: the principal cannot fully monitor or understand the agent's behavior or capabilities. Solutions include enhancing transparency, shortening communication chains, and introducing external oversight mechanisms.
2. Goal misalignment: the agent's actions may not align with the principal's objectives. Solutions include performance-based incentives, long-term contracts, reputation-based rewards, and reducing conflicting goals (e.g., avoiding assigning agents unrelated tasks simultaneously).
3. Cost of supervision: monitoring the agent's behavior requires resources. Solutions involve finding the balance where the marginal benefits of oversight equal the marginal costs, using data to improve monitoring efficiency, and involving multiple stakeholders in oversight.

Tackling these challenges is essential for achieving more efficient and equitable policy implementation.

Literature Review

Information asymmetry exists as a challenge in principal agent relationship, because agents often know more than principals, which makes it hard to monitor their actions and makes self-serving behavior possible. Lane (2013) discussed this problem in New Public Management (NPM). He suggested that short-term contracts (originally designed to improve efficiency) often makes agents even more capable using their knowledge to take advantage of

the principal. He called for transparency and performance audits as solutions. Similarly, Maggetti and Papadopoulos (2018) found that regulatory agencies often use their knowledge to help private interests instead of serving the public (a problem called regulatory capture) .Pollack (2006) explained how information asymmetry affects international delegation, especially in the European Union (EU). Organizations like the European Commission have detailed knowledge about how policies are implemented, while member states often do not. This gives these organizations more freedom to act, which can lead them to stray from the goals of member states. In research policy, Braun and Guston (2003) found that politicians often use their knowledge advantage to distribute resources in ways that benefit themselves or their supporters. They called for independent oversight bodies to review these decisions and ensure fairness. Likewise, Rose-Ackerman (1978) studied corruption and showed how unchecked power allows officials to misuse public funds, and she stressed the need for transparency methods and public involvement as preventions.

The challenge of different goals also appears in different domains that has policy-related principal agent relationships. Lane (2013) said that goal misalignment often arises when bureaucracies or contractors focus on their financial or institutional interests instead of public service objectives. He suggested using performance-based contracts to better align priorities as a workable solution. Also, Maggetti and Papadopoulos (2018) discussed within the domain of regulatory agencies. They found that misalignment would happen if agencies follow their own agendas or favor industry stakeholders over the public good.They suggested balancing agency independence with accountability to make sure they focus on the right goals. In the European Union, Pollack (2006) point out conflicts between member states and supranational institutions: member states often focus on protecting their national sovereignty, while supranational institutions focus more on the greater integration. He suggested using tools like sunset clauses or regular reviews to help manage these disagreements. Braun and Guston (2003) found that in research policy, political leaders sometimes use funding to support their personal or party interests instead of addressing broader societal needs. They called for clearer rules and independent evaluations as fixation. Rose-Ackerman (1978) connected goal misalignment to corruption, showing how agents can prioritize their own interests over the public good. She stressed the need for strong legal systems and strict enforcement to reduce these problems.

The cost of supervision has also been discussed by previous policy scholars in various perspectives. Lane (2013) discribed the trade-off between the benefits of closer monitoring and the additional administrative burden it may create. He suggested to use technology to provide more efficient oversight. Maggetti and Papadopoulos (2018)showed the high costs of supervising independent regulatory agencies, especially when their work spread among different sectors. Doing performance reviews and involving stakeholders are their suggested ways to improve efficiency. Pollack (2006) pointed out that supervising supranational institutions in international governance requires a lot of resources. Their complex tasks make oversight costly. He recommended that member states share these costs by working together, using tools like joint decision-making. In the field of research policy, Braun and Guston (2003) wrote about how supervision costs can make oversight less efficient. They suggested

to focus resources on projects with higher risks or stakes. Rose-Ackerman (1978) emphasized that corruption can make supervision especially costly in developing countries, as there the institutional capacity is very limited. As solution for reducing costs, she suggested to use civil society and media as indirect monitor methods.

Scholars have looked beyond the three main elements to explore other factors that affect principal-agent relationships in specific cases. Maggetti and Papadopoulos (2018) studied how formal authority and informal norms interact, and found that trust and reputation are important in solving agency problems. Pollack (2006) introduced the idea of multilevel governance, showing how multiple principals and agents interact at different levels of decision-making. This paper also mentioned the first weakness in the traditional PA framework, which is it struggles to deal with the complex and changing relationships in real-world policy environments. Other than that, the theory also assumes that principals and agents are rational and focused on maximizing utility, but this often doesn't apply in political situations influenced by social and behavioral factors (Rose-Ackerman, 1978). Other critiques include that the framework ignores informal norms and relationships that shape how policies are implemented and governed (Maggetti and Papadopoulos, 2018).

Case and Analysis

introduction of the case

A representative example of the ethical challenges in handling healthcare data is the 2020 Vastaamo data breach in Finland(*Finland Shocked by Therapy Center Hacking, Client Blackmail | AP News*, 2020). Vastaamo was a private psychotherapy service provider with 25 therapy centers across the Nordic region. It operated as a sub-contractor for Finland's public health system. During the breach, hackers infiltrated Vastaamo's database and stole the sensitive mental health records of over 30,000 patients, including diagnostic details and therapy notes. These stolen records were then used to blackmail both patients and institutions, with some even being sold online. The extreme sensitivity of the leaked information led to devastating consequences, including multiple suicides among the victims(Ghanbari & Koskinen, 2024).

Following the breach, Vastaamo was accused of failing to protect its clients' data adequately and declared bankruptcy in 2021. In February 2023, the perpetrator of the attack was arrested, and by 2024, Alexander was sentenced to six years and three months in prison(Tanner, 2024). This incident prompted the Finnish government to accelerate legislative reforms, including allowing citizens to change their personal identity codes—a key identifier for accessing public and private services—if they faced significant risks of identity theft due to data breaches.

Introduction of related policies

According to the Data Protection Ombudsman's Office (*Data Protection Legislation*, n.d.), Finland has three main pieces of legislation related to data protection: the EU General Data Protection Regulation (GDPR), the Law Enforcement Directive (EU 2016/680), and the Data Protection Act (1050/2018). The following provisions from these documents are relevant to our Vastaamo case:

Firstly, there are provisions about data protection for health data. Laws around health data are strict about how it can be used and they demand strong justifications for processing it:

1) GDPR Article 9: Health data is labeled as "special category data", meaning it's heavily restricted. Processing it is only allowed if:
    a) The person clearly consents (Article 9(2)(a)).
    b) It's necessary for medical purposes or healthcare services (Article 9(2)(h)).
    c) It's for significant public health reasons (Article 9(2)(i)).
2) Law Enforcement Directive, Articles 8 and 23: it defines health data as sensitive and allows processing only if there's a clear legal reason, or the person gives consent. It includes information about health conditions or medical care.
3) Data Protection Act (1050/2018), Section 6: it limits processing health data to specific uses, such as healthcare, research, or statistics. It also requires safeguarding methods , details will be mentioned in 3) of the next paragraph.

Secondly, there are provisions about measures to secure and prevent: the laws require strong technical and organizational measures to keep data safe.

1) GDPR Article 32: data controllers and processors must
    a) use encryption and pseudonymization to secure data.
    b) Make sure data processing systems remain confidential, intact, and available.
    c) Regularly test their security systems and update them as needed.
2) Law Enforcement Directive Article 8: it calls for additional protections for sensitive data like encryption.
3) Data Protection Act (1050/2018), Section 6: it talks about specific steps for health data, such as:
    a) Needs to prevent unauthorized access.
    b) Keeping track of who has accessed, edited, or transfered data.
    c) Regularly test the effectiveness of security measures.

Thirdly, all three documents writes about what to do if a data breach happens:

1) GDPR Article 33: controllers must inform the supervising authority within 72 hours if a breach could be harmful to people's rights. The report should cover the following topics:
    a) What happened and what type of data was involved.
    b) How many records were affected.

    c) Possible consequences.
    d) Steps taken to fix the issue.
2) GDPR Article 34: if the breach could be very risky for individuals, the controller must notify those who can be affected quickly, and explain what happened and what they can do.
3) Law Enforcement Directive Article 33: the breaches with potential risks (e.g. identity theft) must be reported immediately, and individuals must be informed if the risk is considered high.

Clarification of the theory

General Clarification

In this case, Finland's public health system served as the principal, and Vastaamo acted as the agent. The incident highlights three major issues in their relationship, as mentioned by Moe's principal-agent theory.

One major problem in this case was information asymmetry. Before the 2022 attack, there had already been two separate breaches in 2018 and 2019. However, Vastaamo did not report these incidents to the GDPR authorities as required. In Finland's public healthcare system, data systems are divided into two categories: Class A and Class B(Ghanbari & Koskinen, 2024). Class A systems are linked to the Kanta system, where all data and features must undergo a thorough review by officials before being integrated into the system(*Psykoterapiakeskus Vastaamo Kasvu Openin Finaalissa Yhteiskuntavastuu Sote Yrityksen Kasvumoottorina*, 2016). Vastaamo, however, was classified as Class B, meaning that system developers only needed to submit a report on how key security requirements were implemented(Kanta.Fi, 2020).This created information asymmetry. The government was unaware of the breaches at Vastaamo, as the company did not disclose them. Furthermore, Vastaamo's response to the breaches—where an internal IT staff member patched the vulnerability—was carried out without consulting the government. This lack of communication and transparency prevented early intervention and missed an opportunity to mitigate the severe consequences of the larger data breach.

The second problem is goal misalignment. The government and Vastaamo had different objectives. The government used subcontractors like Vastaamo to reduce its own costs and quickly fill gaps in mental health services, which were urgently needed since mental health issues cost society an estimated $1 billion in lost productivity each year(Stt, 2024). The Ministry of Social Affairs and Health's main goal is to promote public health and protect the well-being of the population in all situations(*Task and Objectives - Ministry of Social Affairs and Health*, n.d.). In contrast, Vastaamo, as a social enterprise, had to balance its social mission with the need to make a profit(Vastaamo, 2019). For example, it reinvested earnings into new therapy centers, free online services, and free counseling to support its growth(*Psykoterapiakeskus Vastaamo Kasvu Openin Finaalissa Yhteiskuntavastuu Sote Yrityksen Kasvumoottorina*, 2016). These different goals led to conflicting views on data safety. The government wanted full transparency about potential data breaches to protect

citizens' rights. However, Vastaamo wanted to maintain its relationship with the government and continue expanding. Reporting a breach could be seen as "bad performance," risking its reputation and future opportunities.

The third problem is supervision costs. Government agencies like public health systems often have limited resources, making it difficult to monitor agents like Vastaamo thoroughly. After the data breach, investigations revealed that Vastaamo failed to follow basic data protection protocols(*Henkilötietojen Käsittelyn Asianmukaisen Turvallisuuden Laiminlyönti Ja Tietoturvaloukkauksesta Ilmoittamatta Jättäminen*, 2021). These included not reporting breaches to authorities on time, lacking records of who had access to data, failing to conduct external audits to assess cybersecurity, and not having an emergency response plan for data breaches. These issues were partly due to Vastaamo's classification as a Class B system. Under this classification, the government relied on reports submitted by the company rather than directly auditing its processes(Kanta.Fi, 2020). While this approach saved resources, it left gaps in oversight, making it easier for critical issues to go unnoticed and increasing the risk of significant failures.

There are another two layers of principal-agent relationships where patients act as the principals and the government serves as the agent. Patients often don't know the details of how the government selects private companies or the terms of those agreements. The government may prioritize saving costs over protecting patient data privacy, creating a conflict of interest. Additionally, patients lack the expertise and resources to monitor government decisions. Besides, Vasstamo as a company and its personeel is another PA relationship. The IT staff were hired on zero-hour contracts and are mainly responsible for developing new features. Not feeling responsible for the company in a long term, they didn't know what needs to be considered to ensure security, nor did they have the incentives to insist bringing up the security issue to the management team if it has decided that it is not the focus(they mentioned Tapio, the CEO, didn't think security was an area worth spending money on).

The three issues—information asymmetry, goal misalignment, and supervision costs—indicate how big data creates challenges for policy making in mental health. These challenges can lead to serious problems such as privacy breaches, and a loss of trust in government systems.

Applying Mishra's paper into Vastaamo's case

In Mishra, Heide, and Cort's paper in 1998, the topic of how information asymmetry creates challenges in multi-level principal-agent relationships was discussed. The framework it brought up is very suitable to be applied on Vastaamo's case, and we will elaborate in the following paragraph.

Firstly, the paper wrote that information asymmetry is a very central issue to many relationships, and adverse selection and moral hazards are two big problems that it may create.

Adverse selection means the result of selection may be different from expectation: ideally, before the trade, principals want to choose an optimal agent, but agents may use information asymmetry to hide information that does no good to themselves, leading to principal's wrong selection. In Vastaamo's case, this issue was clear. The company's CEO Ville Tapio, built the system that stored sensitive patient data himself, despite being a self-taught programmer with no formal training in software security (Hämäläinen and Rummukainen, 2020). No outside experts were hired to check if the system met basic security standards, which left serious vulnerabilities unchecked. The government, acting as the principal in this relationship, wasn't made aware of these issues and didn't have way to evaluate the company's true capabilities. Because of information asymmetry, the government chose Vastaamo and gave it full power to manage its highly sensitive health data, without realizing the risks involved.

Moral hazard happens after the principal-agent relationship is built: agent may hurt principal's interests by lowering the quality of service or not being fully responsible (or something else), because of inadequate supervision. In Vastaamo's case, as it belongs to classB（a self-reported system）rather than classA（where stricter supervision by government is conducted）, its irresponsibility was not observed intime.：the company did not inform authorities immediately after detecting the breach, as regulations required; there was no documentation tracking who had access to the system or who had their access revoked; additionally, the company didn't do any external audits to assess its cybersecurity readiness or identify vulnerabilities. Vastaamo also didn't do well as required in terms of having a proper incident management procedure. Although an investigation found a document called "Psychotherapy Center Vastaamo Oy's Actions in a Data Breach Scenario," it did not say anything about steps for preventing, reporting, and recovering from breaches (FINLEX, 2021), which makes it an unqualified document.

Secondly, the paper also explained how information asymmetry may cause issues in multi-level principal-agent theory. Applying the framework to our cases, the ultimate principal are the citizens(including citizens who receive mental healthcare service from Vastaamo), and the government together construct the first principal agent relationship. The government and Vastaamo construct the secondary principal agent relationship. The Vastammo as company and the personeel it hires construct the third PA relationship. All three relationships can be faced with issues caused by information asymmetry, and it will intersect and spread on every participant of the relationship, eventually does harm to the principal: patients assume that the government will choose the most reliable agent, and the government assumes that Vastaamo will comply with data security regulations. However, the trust in both relationships was abused by information asymmetry, leading to the eventual data breach. Eventually, not only do patients lose data privacy, but they also face real financial(being blackmailed) and psychological losses(trauma of fearing the leak of mental health records as they may contain the deepest concern of a human being) as a result of the agency issues between the government and Vastaamo.

To address this issue, mishra et al. introduced two methods.

At the supplier-customer level(in our case government-citizen level), suppliers(government) need to provide clear and trustworthy signals to show their reliability to customers(citizen). For example, government can include third-party certifications or quality assurance clauses in contracts for class B service providers, or it can also reveal the non-confidential part of the contract to citizens to make the signals more reliable.

At the supplier-employee level (in our case government-Vastaamo and Vastamoo-employee level), it is important to have incentive methods, such as performance-based pay, comprehensive training programs, and internal supervision. For example, the government can design a training agenda and incorporate cases about what a government-contracted entities should do when data breach or any other security-related problem happens. The training can also introduce how government and company have worked together to conquer the challenges and prevent negative influence when incidents happen. By emphasizing their partnership rather than framing it as just a supervisory relationship, it builds trust and encourages companies to cooperate more willingly with the government if sensitive data breaches happen in the future.

Challenges to the theory

Although Vastaamo's case clarifies the agent-principal theory in most situations, it also reveals the limitation of it.

The first challenge comes from the complexity of technology. PA theory suggests that principal can manage agent via well-designed contract and supervision, but Vastaamo's case indicate that sometimes the technology that the principal want to supervise is too niche and complicated for non-experts, that they may not be able to develop the most effective supervision strategy. For example, although the government has requested for yearly report and specified the content to be covered, it still didn't discover the risk of data leak. This could indicate that the question is not well-designed enough to indicate possible signs of risks.

The second challenge is that in real life there is often multi-level PA relationships(like Vastaamo), while the traditional PA theory didn't cover this part. Luckily we have other scholars who expanded the theory to situations where multiple PA relationships exist(such as Mishra's paper).

The third challenge is that traditional PA theory put more emphasis on economical efficiency and incentives, but when it comes to data breach about health data, we also need to stress topics like social trust or mental trauma. Other theories that can make up the insufficiency of this area needs to be incorporated as theoretical backup if we want to make true impact by developing new policies.

A fourth limitation of PA theory is its lack of adaptability to real-world deviations from rational behavior. In the Vastaamo case, the company consistently chose short-term cost-saving measures over long-term security investments, such as employing part-time IT personnel on zero-hour contracts and skipping external security audits. These decisions were

not purely about maximizing utility but reflected organizational short-sightedness and a misjudgment of risks. For the government as the principal, the absence of measures to detect these red flags also points to an over-reliance on the assumption that agents will act rationally within their own self-interest. This highlights the need to expand the theory to account for behavioral factors, like bounded rationality, and to develop proactive safeguards against these common lapses in judgment.

Lastly, the Vastaamo case demonstrates the theory's failure to leverage emerging technologies for oversight. Despite the government requiring annual reports from Vastaamo, these static and self-reported updates failed to capture critical vulnerabilities that led to the breach. If the PA framework had incorporated tools like automated auditing, blockchain for transparent data tracking, or AI-based systems to flag anomalies in real time, the government might have detected these risks earlier. For instance, blockchain could have provided an immutable record of access logs, ensuring accountability for who accessed sensitive patient data. Similarly, AI-driven analysis could have identified unusual patterns, such as repeated access attempts from suspicious IP addresses. These technologies offer more than just efficiency—they provide dynamic oversight tools that directly address the complexity of modern data systems. Incorporating these innovations into the PA framework is essential to making it relevant for the challenges of today's digital governance.

After the breach

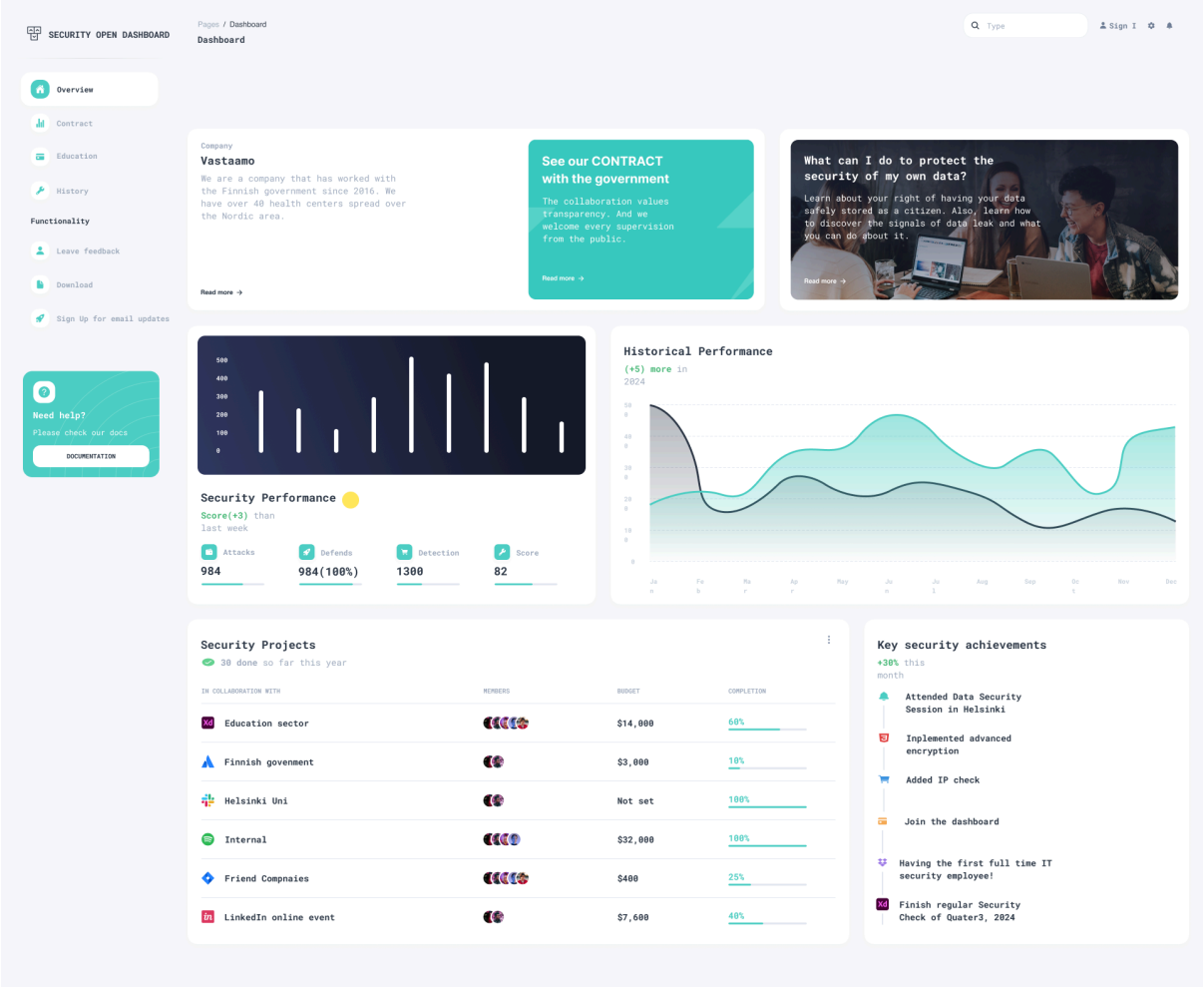
After the breach, the government introduced several measures(Ralston, 2020; *Ohisalo: Finnish Government to Talk About Hacking on Wednesday*, 2020):

1. Agencies were required to ensure the secure handling of personal data to minimize leaks.
2. Departments conducted internal reviews to improve data protection.
3. A new criminal law was introduced to penalize privacy violations.
4. Citizens were allowed to change their personal identity codes in cases of high-risk data breaches.

Using Moe's solutions, we can analyze how the Finnish government responded to the Vastaamo data breach by addressing agency problems and ethical risks in data-driven policymaking. These policies improved transparency and oversight in some ways. For example, allowing identity code changes (measure 4) gave citizens a clear process to protect themselves after a breach, reducing information asymmetry between individuals and the government. The new privacy law (measure 3) improved supervision between the government and private companies by making data protection a top priority, encouraging businesses to enhance their security measures.

However, these actions mainly address existing problems and relationships. They do not provide innovative solutions to fix deeper issues like information gaps, conflicting goals, or ineffective supervision.

Technical Solution



The prototype of Security Open Dashboard

As Mishra et al. mentioned in their paper, technology can be useful as method to enhance transparency, and I would propose building up a dashboard to support regular updates and involve more people in supervision, so that companies that belong to class B can be more secure. The dashboard will be open to public(to monitor, provide feedback, and report any concerns.), implemented by the government, and updated by the companies. Technology-wise, blockchain technology could be integrated to enhance the reliability of the dashboard: reports submitted by companies and updates from the government would be stored on a blockchain to ensure data integrity and authenticity. Also, any changes to the records would generate a timestamp and can be accessible by the public. Citizens could also verify the data's source using blockchain.

The dashboard will display various types of information to increase transparency and accountability:It would make non-sensitive parts of government contracts with companies

publicly accessible, such as project goals, timelines, and funding allocations. Also it will include clear explanations of why specific companies(e.g.Vastaamo) were selected as government partners. Companies would be required to submit quarterly updates instead of annual reports, and the updates will include answers to specific, predefined questions to ensure clarity and detail, rather than submitting a whole report that prioritise organicity. Detailed questions may include, for example, whether the company experienced hacking attempts, how many were successfully blocked, whether there was suspicious IP activity, and what progress had been made in solving previously-reported security issues. The dashboard would also include a feedback and complaint section where citizens are able to report potential issues, such as receiving spam emails or suspicious calls after interacting with the company, which would help identify unreported data breaches and give timely warning.

It would also be nice to have a risk monitoring feature. We can use a color-coded system—such as green, yellow and red—to show the current risk level of a company based on its compliance and safety record(which can be decided by the government based on the company's quarterly report). Other dimensions to consider can be: how many security audits the company has completed, how often do employees receive cybersecurity training, and whether the company has implemented important measures like encryption. High-performing companies can be recognized with awards, such as a "Data Security Excellence" badge, which will be highlighted on the dashboard. This would exert as incentives and motivate other companies to also improve their standards.

Another important feature could be an education section for the public. This section targets the citizens, and would provide easy-to-understand resources on data privacy and security, such as short videos or interactive lessons. The main goal of this is to teach people how to discover signs that indicates their information might have been leaked(like suddenly getting lots of spam emails or strange phone calls), and guide them on how to report these issues through the dashboard.

To make all of this work, modern technology needs to be used. The dashboard's design can be made user-friendly by using stacks like React.js, so it's easy to use on phones and computers. Python or Node.js could be used to manage the system's backend, while databases like PostgreSQL or MongoDB would store the information, the specific choice also depends on the government's preference. To keep sensitive data secure, encryption and blockchain will be used, as mentioned before. Also, strict access controls would make sure only authorized people can make changes. Additionally, small added tools like D3.js could create simple charts and graphs to help citizens easily understand the data, while systems like ELK stack would track and log activity for transparency.

To conclude, a dashboard would make government and company processes more open and easier to understand. By using blockchain for security, providing section about educational resources, and rewarding companies for what they have done well, it would help everyone take data security more seriously. It would also give citizens a way to actively participate in keeping the system accountable and safe.

Conclusion

The Vastaamo case shows the ethical and practical challenges of using data in mental health policymaking. While the Finnish government took steps to improve oversight and privacy protection, there are still some improvements that can be made based on suggestions from principal agent theory and its expansions. PA theory provides a useful theoretical framework to analyze this issue, and it is made clear that solutions that addresses goal misalignments, inefficient supervision, and especially information asymmetry needs to be brought out. A dashboard was proposed as one of the possible solutions to tackle information asymmetry. Despite all the evidence that Vastaamo speaks to the theory, we also need to see how it challenges the PA theory, which are caused by the complexity of technology, multiple PA relationships happening at the same time, and the inherent limitations that PA carries with itself.

References

[1]*The rise of digital health technologies during the pandemic | Think Tank | European Parliament*. (n.d.). https://www.europarl.europa.eu/thinktank/en/document/EPRS_BRI%282021%29690548

[2]Watson, E., Fletcher-Watson, S., & Kirkham, E. J. (2023). Views on sharing mental health data for research purposes: qualitative analysis of interviews with people with mental illness. *BMC Medical Ethics*, *24*(1). https://doi.org/10.1186/s12910-023-00961-6

[3]*Stigma, Prejudice and Discrimination Against People with Mental Illness*. (n.d.). https://www.psychiatry.org/patients-families/stigma-and-discrimination

[4]Jensen, M. C., & Meckling, W. H. (1976). Theory of the firm: Managerial behavior, agency costs and ownership structure. *Journal of Financial Economics*, *3*(4), 305–360. https://doi.org/10.1016/0304-405x(76)90026-x

[5]Moe, T. M. (1984). The New Economics of Organization. *American Journal of Political Science*, *28*(4), 739. https://doi.org/10.2307/2110997

[6]*Finland shocked by therapy center hacking, client blackmail | AP News*. (2020, October 26). AP News. https://apnews.com/article/psychotherapy-cabinets-finland-6b27c895df0abd532a4fb000c9d5d517

[7]Ghanbari, H., & Koskinen, K. (2024). When data breach hits a psychotherapy clinic: The Vastaamo case. *Journal of Information Technology Teaching Cases*. https://doi.org/10.1177/20438869241258235

[8]Tanner, J. (2024, April 30). *Finnish hacker imprisoned for accessing thousands of psychotherapy records and demanding ransoms | AP News*. AP News. https://apnews.com/article/finland-court-hacking-ransom-psychotherapy-center-b03183e5ca66a768d743f7e84b368829

[9]Hiilamo, E. A., and L. Kukkonen. "Psykoterapiakeskus Vastaamolla on alan silmissä kehno maine: Harhaanjohtavaa mainontaa, painostusta ja” härskiä toimintaa”." *Helsingin Sanomat* 27 (2020).

[10]Kanta.Fi. (2020, June 2). Latest Kanta services have been certified. *Kanta.fi*. https://www.kanta.fi/en/notice/-/asset_publisher/cf6QCnduV1x6/content/myos-uusimmat-kanta-palvelut-ovat-saaneet-sertifioinnin

[11]*psykoterapiakeskus vastaamo kasvu openin finaalissa yhteiskuntavastuu sote yrityksen kasvumoottorina*. (2016). suomalainentyo.fi.

[12]Stt. (2024, August 28). Kela: Mental health sick leaves cost Finland €1b annually. *News*. https://yle.fi/a/74-20107799

[13]Vastaamo, P. (2019, March 5). *Psykoterapiakeskus Vastaamo Toimintakertomus 2018* [Slide show]. SlideShare. https://www.slideshare.net/slideshow/psykoterapiakeskus-vastaamo-toimintakertomus-2018-134744561/134744561

[14]*Task and objectives - Ministry of Social Affairs and Health*. (n.d.). Ministry of Social Affairs and Health. https://stm.fi/en/ministry/task-and-objectives

[15]*Henkilötietojen käsittelyn asianmukaisen turvallisuuden laiminlyönti ja tietoturvaloukkauksesta ilmoittamatta jättäminen*. (2021). https://finlex.fi/fi/viranomaiset/tsv/2021/20211183.

[16]Ralston, W. (2020, December 9). A dying man, a therapist and the ransom raid that shook the world. *WIRED*. https://www.wired.com/story/finland-mental-health-data-breach-vastaamo/

[17]*Ohisalo: Finnish government to talk about hacking on Wednesday*. (2020, October 26). Helsinki Times. https://www.helsinkitimes.fi/finland/finland-news/domestic/18209-ohisalo-finnish-government-to%20-talk-about-hacking-on-wednesday.html

[18]Lane, J. (2013). The Principal-Agent Approach to Politics: Policy Implementation and Public Policy-Making. Open Journal of Political Science, 03(02), 85–89. https://doi.org/10.4236/ojps.2013.32012

[19]György, A. (2012). Public Sector's Principal-Agent Theory in a Global World. POLITEJA, 9, 101–107. http://cejsh.icm.edu.pl/cejsh/element/bwmeta1.element.desklight-05cc0ec5-57f6-4aa5-9042-7d1f5c9b9068

[20]Groenendijk, N. (1997). A principal-agent Model of corruption. Crime, law and social change, 27(4), 207-229. https://doi.org/10.1023/A:1008267601329

[21]Pollack, M. A. (2007). Principal-Agent Analysis and International Delegation: Red Herrings, Theoretical Clarifications and Empirical Disputes. SSRN Electronic Journal. https://doi.org/10.2139/ssrn.1011324

[22]Maggetti, M., & Papadopoulos, Y. (2016b). The Principal–Agent Framework and Independent Regulatory Agencies. Political Studies Review

[23]Mishra, D. P., Heide, J. B., & Cort, S. G. (1998). Information Asymmetry and Levels of Agency Relationships. *Journal of Marketing Research*, *35*(3), 277–295. https://doi.org/10.1177/002224379803500301

[24]*Data protection legislation*. (n.d.). https://tietosuoja.fi/en/legislation.

[25]*Data Protection Act*. (2018). https://www.finlex.fi/en/laki/kaannokset/2018/en20181050.pdf.

[26]*General Data Protection Regulation*. (n.d.). https://eur-lex.europa.eu/legal-content/EN/TXT/?qid=1528874672298&uri=CELEX%3A02016R0679-20160504.

[27]*Law Enforcement Directive (EUR-Lex)*. (2016). https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016L0680.