Information Commissioner's Office

Data Controller Study 2025

Qualitative findings report

Economic analysis

June 2025

ico.
Information Commissioner's Office

Contents

1. Background

In February and March 2025, IFF conducted 20 qualitative follow-up interviews with organisations that participated in Year 2 of the Data Controller Study survey.

The interviews were focused on the use of technological processes to process personal data. These processes included anonymisation, pseudonymisation, artificial intelligence (AI), automated decision making (ADM), biometrics and facial recognition technology.

This document summarises the key findings from the interviews. Although the small sample size means that we should be careful when generalising the findings, the summary of the main themes of the responses provides valuable additional insight to the Data Controller Study. The key themes across all technologies are summarised below:

- **Familiarity and uptake of the technologies is generally low:** Whilst anonymisation, pseudonymisation and biometrics were relatively well understood concepts, only a small proportion of data controllers used these processes. In contrast, many respondents reported low levels of understanding of AI and ADM, stating that they do not understand the full potential of these technologies.
- **Organisations reported feeling more secure with certain technologies in place:** Biometrics were used to restrict the unauthorised access and improve the storage security of data, whilst anonymisation and pseudonymisation could limit the harms of unintentional data breaches.
- **Anonymisation and pseudonymisation encourage data sharing:** most organisations using anonymisation or pseudonymisation used these processes to allow them to share information with other organisations and the public without revealing personal data. Respondents also reported that citizens would be more willing to share information when they believe it is stored in a way that it cannot be attributed to them.
- **The adoption of technologies can drive efficiency:** technology and the digitalisation of data has improved like speed and accuracy with which organisations can anonymise and pseudonymise data. In addition, many respondents reported that the use of AI or ADM could free-up valuable employee time on admin and research tasks.

- **Ensuring suitable staff training and awareness is a key challenge:** Many organisations reported concerns around employees using tools such as AI or ADM in an inappropriate fashion. Some organisations reported that the decisions they make are too complicated and nuanced to be left to ADM or AI and others were worried about the accidental egress of personal data through AI or ADM models made available online or through legacy software. As a result, ensuring suitable training on secure data management was highlighted by many respondents as a primary concern, particularly when sensitive data is processed.
- **Future uptake is uncertain:** Most organisations did not expect an increase in the use of anonymisation, pseudonymisation or biometrics. Many reported technological maturity and costs as leading factors that would determine the future uptake. However, organisations had diverging views on the future adoption of AI and ADM. Many stated they would not consider this technology in the future, whilst others expressed the views that the increased use would be inevitable.

As the organisations covered a range of activities and sizes, it is important to note that the scale of data processing, and the data subjects this relates to, vary across the interviews. Some of the respondents dealt with all of the data processing discussed themselves, others employed third party services, which aided in the management and security of data within the organisation.

The Technical Report published alongside the Data Controller Study details the methodology underpinning the Study and provides supplementary information about the methodology followed for the qualitative interviews.

2. Anonymisation and pseudonymisation

2.1. Understanding and uptake

Anonymisation and pseudonymisation are ways of reducing risk and improving security when processing personal data by replacing or removing information that identifies people.

In our guidance, we define anonymisation and pseudonymisation as follows:

Anonymisation is the process of turning personal data into anonymous information, so that it then falls outside the scope of data protection law. Data is anonymised when it does not relate to an identified or identifiable individual or is rendered anonymous in such a way that individuals are not (or are no longer) identifiable.

Pseudonymisation is the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

Our quantitative survey revealed that 7% and 3% of UK data controllers respectively reported using anonymisation or pseudonymisation when processing personal data.

As we were particularly interested in the insights of organisations using the technologies of interest for our qualitative interviews, we targeted respondents that reported using the specific technologies in the qualitative survey. As a result, our sample captured 17 organisations that reported using either anonymisation or pseudonymisation techniques to process personal data in the quantitative survey. However, throughout the completion of the qualitative interviews, we noted that not all organisations use of the technologies aligned with our expectations.

For example, whilst anonymisation and pseudonymisation were generally well understood by most respondents, one respondent reported that their data was "completely anonymous because it's behind a firewall, which can only be accessed by me and can't be accessed by anyone else",

suggesting that there may be some uncertainty amongst organisations about the process of data anonymisation.

2.2. Anonymisation and pseudonymisation enable data sharing

The majority of organisations adopting anonymisation or pseudonymisation processes did so in order to enable data sharing outside of their organisation.

Several Councils noted they had policies to redact personal information for any output issued to the public, unless specific permission from the individual to publish the information has been obtained. This included the publication of consultation responses and performance reporting to central government.

For several organisations processing medical personal data, anonymisation allowed them to complete research and report cohort findings while maintaining confidentiality of their patients. Several organisations also reported that anonymisation helped their organisations keep data for longer and allowed for the reuse of data for other research purposes.

Dyslexia charity

Non-profit charity organisation, 2-9 employees

A charity raising awareness and support for people in Scotland living with dyslexia highlighted the benefit that anonymisation has brought to their organisation.

For the last 20 years, they have fielded a survey across people with dyslexia. By anonymising the findings, the organisation has been able to share insights and raise awareness of the dyslexic community and their experiences, whilst maintaining the privacy of individuals.

The organisation noted that this allows members of the public to trust them as an organisation: "People know we are trustworthy, reliable and credible in terms of recognising our duty to be compliant [with the GDPR]".

Effective anonymisation also helps public sector bodies meet their regulatory obligations, particularly those set out by the Freedom of Information Act 2000 (FOIA), in line with data protection law. The FOIA entitles members of the public to request information from public

authorities and obliges public authorities to publish certain information about their activities. Organisations reported that anonymisation made it possible to disclose information to the public under FOIA without risking the identification of individuals.

2.3. Balancing the right to data access with data protection

One of the challenges respondents raised around anonymisation was determining the appropriate level of redaction, stating that in certain circumstances, there was uncertainty about what data to anonymise when.

Freelancing film and editing company

Private sector, 0-1 employees

Film and production companies collect personal identifiers such as faces and voices as part of their work. This sometimes includes the faces of individuals in the background of shots. Where consent from these individuals has not been obtained, organisations will blur out the subject's face in post-production as means of anonymisation.

The respondent raised two key challenges. Firstly, the process to anonymise faces was manual and involved tracking faces across the screen. Secondly, the organisation reported that this process was done subjectively, without a strict threshold distance at which to blur individuals, with the organisation therefore unclear of whether they were making more edits than required to meet their compliance responsibilities.

Other organisations welcomed more guidance from the ICO about how to balance the right to access information in FOIA requests with data protection requirements. For example, a medium-sized organisation responsible for overseeing local mental health services and a local authority stated that they faced issues with stakeholders wanting more disclosure under the FOIA than what the organisation deemed appropriate under data protection regulations.

2.4. Anonymisation and pseudonymisation increase public trust

One of the key benefits of anonymisation and pseudonymisation mentioned in the interviews was the increase in public trust. Organisations reported that these processes helped develop a trusting

relationship between the organisation and the public, where citizens were confident that their data was being treated in a secure manner. This was particularly prominent acrosspublic sector organisations, like local authorities and town councils, who used anonymised or pseudonymised data to report outcomes back to their citizens.

Local authority town council

Public sector, 2-9 employees

A local town council implements pseudonymisation to update their citizens regarding allotment allocations. Applicants are issued a unique number on the council website and can use this to track their place on the waitlist.

The town council reported that this has positively impacted the community, with residents feeling confident that they are being treated fairly in relation to allotment waiting lists and allocations.

"[People are] interested to know that it is being dealt with fairly and transparently."

Several public sector authorities also noted that the anonymisation or pseudonymisation of data helped increase citizen engagement. For example, organisations noted that citizens were more likely to provide feedback or respond to public consultations when they were sure that responses would be treated with confidentiality and anonymised before publication.

Small town council

Public sector, 2-9 employees

This town council reported anonymising consultation responses before publication. This was done by manually deleting names and other identifying information from documents and spreadsheets.

"You've got to be careful with that data because […] depending on what you're consulting on, people could work out who's saying it […] and if someone's particularly supportive for it, then they could get a lot of grief."

They reported that this process of anonymisation increased citizen's trust and encouraged residents to share information with the council with the confidence that it won't be attributed to them.

"If they know that they're not going to be shared more widely or pinpointed that it comes back to them, I suppose it might encourage more people to engage with us."

The council noted that this increased engagement has provided valuable feedback which has helped them improve their services.

2.5. Uptake of specialist software is limited

Throughout the qualitative interviews, several organisations referred to manual processes for anonymisation, including "blacking out" text in PDF documents or "literally deleting columns from spreadsheets".

Organisations reported how helpful the digitalisation of data was to improving their process for anonymisation, particularly for large volumes of personal data. Several organisations highlighted the time-savings efficiency that programmes such as Adobe and Excel have brought about compared to the past where documents had to manually be covered and photocopied. In addition, one public sector organisation reported that the primary benefit of using such digital programmes was the reduction in accidental disclosure of data due to human error.

Many organisations noted that more advanced anonymisation software, including those with AI functionality, could be used to improve the efficiency of their anonymisation process. Out of the 15 organisations identified as using anonymisation or pseudonymisation, seven reported that their use would likely increase in the future. Of these, five noted their interest in securing anonymisation tools with greater functionality or AI enhancements. Whilst some organisations were actively considering more specialist software, challenges around costs of these programmes and maturity of AI technology were reported.

Government body

Public sector, 250+ employees

"We've had demos of some [] really good tools that could help the process, but money is always an issue. [T]here's the tools that look as though they could save an awful lot of work and time, but we can't. [W]e haven't got a budget for that."

3. Artificial Intelligence (AI)

3.1. Understanding and uptake of AI is still limited

Responses from the qualitative interviews highlighted large knowledge gaps around AI, its use cases and benefits. The ICO guidance provides the following definition for AI:

> We use **Artificial Intelligence** (AI) as an umbrella term for a range of algorithm-based technologies that solve complex tasks by carrying out functions that previously required human thinking.

In the qualitative interviews, six respondents self-reported a "basic" or "low" understanding of AI, with one organisation reporting they did not know what AI was. Many respondents referred to generative AI models or chat bots when asked to define AI. More advanced responses included reference to the "use of algorithms", "non-human" or "automated" data use and "computer learning".

These relatively low levels of understanding could, in part, explain the limited adoption of AI across organisations. In our quantitative survey, 8% of organisations reported using AI when processing personal data. Within our qualitative interviews, most organisations reported having AI software in place for staff to use. However, only three organisations reported using AI for the purposes of processing personal data. This included a film and production company for audio-enhancements, a collection of councils for the allocation of imported data into data cubes and a local council for generating meeting minutes.

> **Medical practice**
>
> **Public sector, 10-49 employees**
>
> "We just don't know enough about [AI]. I think that's the main thing. We don't understand and we've not had any training on it."

Organisations using AI for purposes other than data processing reported using AI for the analysis of large data sets (scientific research organisation) or the detection and prevention of cheating or anomalous behaviour in remote examinations (membership organisation for medical practitioners). Other organisations reported access to different generative

AI software that was made available for their employees, for the purposes of drafting and generating notes.

3.2. Efficiencies are quoted as the primary benefit of AI adoption

The primary expected and reported benefit of adopting AI was time saving efficiencies. For example, several organisations reported the potential to save employee time when writing up notes, collating meeting minutes or undertaking research activities. One organisation pointed out that their use of AI to summarise regulatory requirements has made some aspects of data processing activities more efficient.

Local council

Public sector, 250+ employees

"It's the next step up from Google in the sense that you, you can ask it a question as opposed to having to research what it is you're looking for and it'll do the research for you."

In the research space, one organisation reported that they could use AI to make better use of large scientific datasets. Another organisation theorised that AI could provide increasing benefits in the medical field for more in-depth analysis of information.

Two organisations also reported the potential for AI to improve accuracy by minimising the element of human error when processing personal data. On the other hand, several organisations highlighted concerns about the accuracy of information gathered by AI technologies. One public sector organisation reported concerns that employees would become over reliant on such technologies and would fail to check outputs. Another noted that incorrect outputs could significantly harm an organisation's reputation.

3.3. Ensuring appropriate training and awareness is challenging

One of the key concerns regarding the adoption of AI was the unconstrained introduction of AI technology. For example, five of the 20 organisations reported that generative AI software had been implemented at their organisation through existing software installed on employee laptops. Organisations noted that the introduction of AI features in legacy software can leave organisations without a chance to properly train employees on data management prior to the launch of the AI technology.

Whilst two organisations reported having taken steps to firewall personal data processing from AI technologies made available to staff, many highlighted the concern around the accidental egress of personal data as employees may lack the proper training to use the AI tools in an appropriate fashion.

Collection of three district councils

Public sector, 50-249 employees

The public sector authority described the adoption of AI as a double-edged sword as data processing tasks become more efficient but present increases the risk of accidental data leakage. In particular, the organisation was concerned about AI technology being introduced without oversight or training:

"[P]roviding everyone with a standing knife on the desk without telling them how to hold it safely is probably one of the most dangerous things the local authority has done. In fact, any business has done. [Generative AI software] has automatically rolled [out] into every single desktop, and it's not something you can stop necessarily. So from a purely governance perspective, it's been a nightmare."

This rapid adoption of AI was seen as particularly risky for organisations that process sensitive data. Several public sector organisations reported concerns that inadequate preparation or staff training could result in sensitive personal data being inputted into unconstrained AI models and thereby shared outside the organisation.

Local council

Public sector, 50-249 employees

"If you look at using [AI] with social care data or children's information within education, clearly you don't want that information seeping out inadvertently into the Internet and learning models."

Whilst no organisations reported actual data egress events, many stated their concern around the adoption of AI without the appropriate staff training.

3.4. Organisations are torn about the future of AI

The qualitative interview respondents were divided around whether the rise of AI was "inevitable" or not applicable to their organisation.

Focussing on the latter first, several organisations reported that they did not adopt AI as their organisations are too small and do not process enough personal data. Even looking to the future, many organisations reported it would be unlikely to adopt AI, stating challenges around the risks of processing sensitive data. One local authority town council stated they "would have to change radically for us to consider it".

Freelance consultant for mortgage advisor firms

Private sector, 0-1 employees

The freelance consultant highlighted that AI was unlikely to provide large benefits to their organisation due to the limited data that they hold: "I don't think that I hold enough personal data that I can't process with the systems that I'm already using."

Whilst they were considering the adoption of AI to write up notes and summaries from meetings, they noted the need to consider the data protection element of any such AI implementation:

"I would need to inform people that I'm recording the meeting and for what purpose…my actual data being held personally may well increase quite substantially if I'm starting to record meetings."

As a result, the respondent noted that their use of AI would be unlikely to change in the future.

The attitudes expressed above in relation to AI could, in part, be driven by the number of organisation with a low understanding of AI and the benefits it could bring, with one respondent from a small town council stating: "I'm not aware of what's available - there could be some really good stuff out there that I should be using." In fact, even those in the early, investigative stages of AI adoption within their organisation were unsure of the potential impacts, with pilot phases being implemented to understand the full "ripples and ramifications".

Government body

Public sector, 250+ employees

The government body is currently undertaking an early pilot to investigate an AI tool to be able to process personal data and have already written an overarching policy on AI use.

"We're not even totally sure what it can do for us at the moment it is such we're in such early stages."

Whilst they have not realised any impacts yet, they are expecting time saving efficiencies and improved accuracy by minimising human error.

They did not face pushback when implementing this pilot, but want to ensure employees are equipped with the appropriate skills to be able to use it to its potential whilst having controls to ensure that the output data is accurate.

"It will never replace a human being because it always needs that human eye to look at what the output data is and make sure it is what you thought it should be."

On the other hand, there were a large number of organisations who reported, with great certainty, that their use of AI would increase. In fact, five organisations described the rise of AI as "inevitable".

Local council

Public sector, 50-249 employees

"No matter how much of a Luddite you are, how much you rail against the use of AI and stuff like that, inevitably all the systems that we are using as they go through iterations, updates and stuff like that, those companies that are providing the systems to you will be sliding AI into their technology… [We need to] make sure that people are aware of what they're doing and also if they are planning on doing it, making us aware so that we can do some due diligence to make sure that we can protect the organisation and the end user."

4. Automated decision making (ADM)

4.1. Understanding and adoption of ADM is limited

The ICO guidance defines ADM as follows:

Automated decision-making is the process of making a decision by automated means without any human involvement. These decisions can be based on factual data, as well as on digitally created profiles or inferred data. Examples of this include:

- an online decision to award a loan; and
- an aptitude test used for recruitment which uses pre-programmed algorithms and criteria.

Organisations that participated in the qualitative interviews had a general understanding of ADM, with several referencing uses cases around loan decisions and job applications as set out in the definition above. Other organisations self-reported low understanding, with three organisations requesting the definition of ADM during the interview.

Adoption of ADM was limited amongst the organisations interviewed, with one respondent from a large public sector body expressing that, as far as they understood it, ADM use was illegal under the UK's GDPR. Only one organisation, a large local government organisation, reported undertaking ADM to process personal data.

Collection of three district councils

Public sector , 250+ employees

The organisation reported using an algorithm-based ADM model to process council tax data for over 150,000 citizens. This process is supported by bespoke software packages developed and delivered by private companies.

The organisation explained that their automated decision making is informed by provisions in statute and government policy that minimise some of the challenges in explaining why certain decisions are taken.

However, the organisation did report challenges around bridging the gap between unrealistic expectations from leadership and the risk of

undermining good data management practices.

Overall, the adoption of ADM was seen as inevitable. The organisation is currently considering the adoption of additional machine learning capabilities into the council tax processing and highlighted that the effective integration will require clear guidelines around AI uptake by the government.

4.2. ADM was not deemed suitable for sensitive decisions

Several organisations noted that their lack of interest in ADM was driven by the sensitive nature of their organisation's work and the type of data that it manages.

Local council

Public sector, 250+ employees

The local council reported that ADM technology was currently not developed enough to make nuanced decisions. As a result, they decided not to implement ADM as their service provision requires delicate decision-making that affects the lives and livelihood of citizens.

However, they noted they would likely adopt ADM in the future, once other organisations had proved its value for making complex decisions. "I think it's probably more for others and then we'll jump on the bandwagon. If it looks like it's going to be successfully useful."

One council stated that the decisions they make are too complicated and nuanced to be left to ADM, which was described as being "not there yet" and "too risky at the minute". Many public sector organisations felt strongly that human judgement was required for their work and that current technology would not be able to replicate this ability to render judgement.

Government body

Public sector, 250+ employees

A government body responsible for a range of services collects personal data of residents to process council tax, educational, employment and healthcare needs, and manage parking and traffic.

They noted that they do not use ADM within their organisation due to the nature of the services they provide as they need to be able to demonstrate an audit trail leading to decisions:

"It's quite difficult for local authority that is so accountable for its decision making to use automated decision making. Because you got to be able to demonstrate how you've arrived at that outcome. And you know, there will always be unique circumstances that have to be taken into account."

As a result, the organisation did not expect their use of ADM to change in the future.

This was despite one organisation speculating that the use of ADM could help avoid or reduce unconscious bias in some decision making.

4.3. Future uptake of ADM may be slow

Of the 20 qualitative interviews, 12 organisations stated they do not see their organisation considering or implementing ADM in the future.

Some organisation stated that this lack of interest stemmed from the perception that the organisation was too small to meaningfully benefit from it.

Town council

Public sector, 2-9 employees

The organisation reported not knowing what ADM was. After being provided a definition, the organisation confirmed they had not adopted any ADM and did not expect any changes in the future:

"We're very old school and a lot of our work is still paper based… we don't use that in anything that we do. I can't think of anything. And I can't think going forward what we would rely on to make that kind of decision in the work that were doing."

Other organisations, however, could see the benefits that ADM could provide to their organisations but were wary of being amongst the first organisations to implement such processes. This included a local council, considering the implementation of ADM for their public service delivery and an NHS general practice, considering the implementation of an online triage system to prioritise appointments.

NHS General Practice

Public sector, 10-49 employees

A medical practice reported that they were considering ADM to introduce an online triage system, where patients go through questions, and the system would provide them with an outcome as to whether they should go to the pharmacy, get an appointment with a GP, or visit a nurse.

They noted that they were aware of other practices already adopting online triage processes, and were keen to observe how other practices implemented their ADM before using it themselves.

"We do keep looking at it and seeing how beneficial it is and were watching other practices…a lot of practices have had kickback and complaints…because I think [patients] just get sick of talking to automated machines. At the moment we're holding back, but we are a medium-sized practice so I can imagine the demand for larger practices and the reasons why they're using it[.] So we are just sitting on the sidelines."

5. Facial and biometric recognition technology

5.1. Use of facial and biometric recognition technology is limited

In line with our ICO guidance, we define biometric recognition technology as follows:

Biometric recognition refers to the automated recognition of people based on their biological or behavioural characteristics.

Our quantitative survey revealed that 7% of UK data controllers reported using facial or biometric recognition technology when processing personal data.

Overall, nine organisations that took part in the qualitative interviews reported using facial or biometric recognition technologies. For the majority (five respondents), this related to the processing of facial or fingerprint data to access work devices like phones and laptops. Other organisations used fingerprint technology to regulate staff access to buildings and facilities.

Computer consultancy

Private sector organisation, 0-1 employees

This organisation reported using facial and biometric recognition technology for improved security. Whilst the business does not process the biometric data themselves, they use facial and fingerprint scanners for security purposes: "If you wanted to access something within a data file for instance, you would need to provide biometrics plus a password."

They reported that they first began using this system 10 years ago and are pleased with the improved accuracy of the technology since then. The organisation noted that the adoption of facial and biometric technology has led to improved customer outcomes: "From the customers point of view, it has made them feel more secure."

5.2. Identification used to drive improved safety

The majority of organisations reported using facial or biometric recognition technology in order to improve safety – whether to restrict access to digital workspaces like phones or laptops or physical access to buildings or forensic analysis. These organisations reported that the use of facial or biometric recognition technology could ensure a more secure and reliable verification of identify to limit unauthorised access. In contrast, two organisations reported using key code or 'smart card' systems for the same purposes, noting that these processes were simpler to implement in comparison to biometric recognition technology.

NHS General Practice

Public sector, 10-49 employees

An NHS general practice was considering the adoption of facial and biometric recognition technology to help eliminate prescription fraud - where individuals fraudulently claim to be a patient in order to obtain prescription drugs.

"We're in a deprived area, we do have a lot of problems with drug seeking behaviour. So a patient at the moment could come in and they could tell us a different name, address, and they can actually go around practices…they'll come in and ask for a certain type of drug…this would be perfect if they had to prove who they were."

However, the organisation reported that they were currently unable to adopt this technology as they are under the obligation to accept all patients, even those without ID, which could limit the effectiveness of the facial and biometric recognition technology.

5.3. Challenges around data sensitivity

Several organisations noted that the sensitive nature of biometric and facial recognition technology made it challenging to adopt. Organisations would need to ensure that the data is being collected and stored in adequate ways. This can make the adoption of such technologies more challenging when compared to other systems. For example, a small town council reported considering the use of facial or biometric recognition technology as part of their building security system. In the end, they decided to use a key code system because it was simpler to implement.

Data analysis, IT and marketing consultancy

Private sector, 0-1 employees

The organisation reported that they saw no need to implement facial or biometric technology within their organisation. Whilst they noted the potential to use FRT to log into accounts, they flagged that they would be unlikely to hold the personal data themselves.

"It's just not something we would want to hold. We don't as a company ourselves [process personal data], we would never really want to have anything to do with the personal data directly."

One organisation in particular reported that overcoming the community's reluctance towards the storing of biometric data would be a key challenge for the wide-spread adoption of such technologies.

5.4. Not many organisations expect to take up facial or biometric recognition technologies

Overall, the majority of organisations reported that they did not expect to adopt facial or biometric recognition technologies in the future. This was driven by the lack of relevant use cases to their organisation.

Freelance compliance consultant for mortgage advisor firms

Private sector, 0-1 employees

The organisation saw no need for the adoption of facial or biometric recognition technology within their business, except for the potential to log into work laptop.

"If I ever needed to implement them, I would be happy to do so but I would probably only be implementing them if I saw great advantage and efficiency. I just don't need it at the moment, I can't think of any scenario. No, my business is very manual in that way rather than digitally orientated, so no, I can't think that I would need to use it."

However, several organisations not currently using biometrics or facial recognition technology reported that they were not opposed to use of the technologies in the future. Whilst many did not name any immediate use cases, some could see themselves using these technologies to ensure personal data is stored more securely. However, many of these

organisations reported that the adoption of these technologies would be contingent on the costs of implementation decreasing. For example, one organisation reported that they had considered adopting multi-factor authentication for staff laptops using FRT, but ultimately chose not to as costs were prohibitive.