BEHAVIOURAL EXPERIMENTS IN DATA PRIVACY

CSBC AND BUSARA RESEARCH | NOVEMBER 2020

IntAct
Data Privacy : Intent to Action

Busara

Centre for Social and Behaviour Change

Acknowledgements
We would like to thank Omidyar Network and Omidyar Network India for their continued support and enthusiasm. Subhashish Bhadra, in particular, provided invaluable guidance. We are also very grateful to our stakeholders - Saranya Gopinath, Aarka, CUTS, Facebook, Dvara, eGov Foundation, Monk Prayogshala, and DSCI who gave us their time, input, and ideas for the interventions we tested.

A big thanks to the Busara and Centre for Social and Behaviour Change teams for their support and hard work on this project. Lastly, we are grateful to our respondents for their time and for making it possible to do what we do.

Team

Busara Centre for Behavioral Economics

James Vancel | *Senior Advisor and Board Member*

Ridhi Podar | *Engagement Director*

Dhwani Yagnaraman | *Associate*

Jaspreet Singh | *Associate*

Centre for Social and Behaviour Change

Pooja Haldea | *Senior Advisor*

Pavan Mamidi | *Director*

Priyanka Goyal | *Marketing Consultant*

Tirtha Patel | *Assistant Manager*

Saksham Singh | *Associate*

TABLE OF CONTENTS

05 Executive Summary

20 The Behavioural Experiment
Experiment design and flow

23 Our Nudges
Design, behavioural underpinning and hypothesis

44 Measuring Privacy
Change in users privacy related behaviours

58 Context is Key
Differences between India and Kenya results

60 Nudging Privacy
Key findings and implications

65 Recommendations and Next Steps

67 Conclusion

Executive Summary

Why we did this research

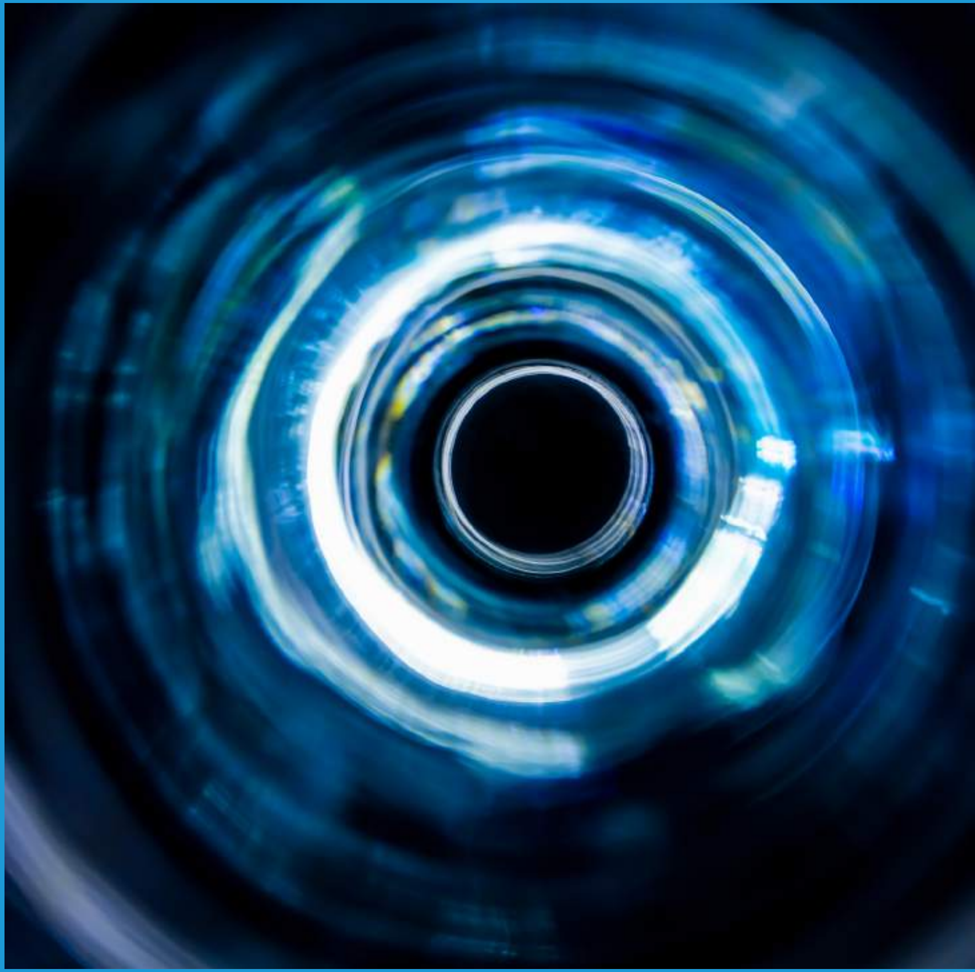
The General Data Protection Regulation in Europe made data privacy a top priority for governments, businesses and individuals. In the Global South, the penetration of technology and internet is rapidly increasing while literacy and awareness levels vary widely. Users would like to protect themselves but falter at the decision making point, lured in by the instant gratification of access to services or apps.

This intent-action gap, along with myopia or present bias exhibited by users, is one of our core challenges as we seek to understand and design solutions to increase user privacy consciousness within the Indian and Kenyan context.

The core research questions we seek to answer are;

- Can users be nudged to be more privacy conscious?
- Can better privacy practices by organisations be a business advantage?

We began with the proven premise that users’ privacy related decisions are impacted by behavioural biases

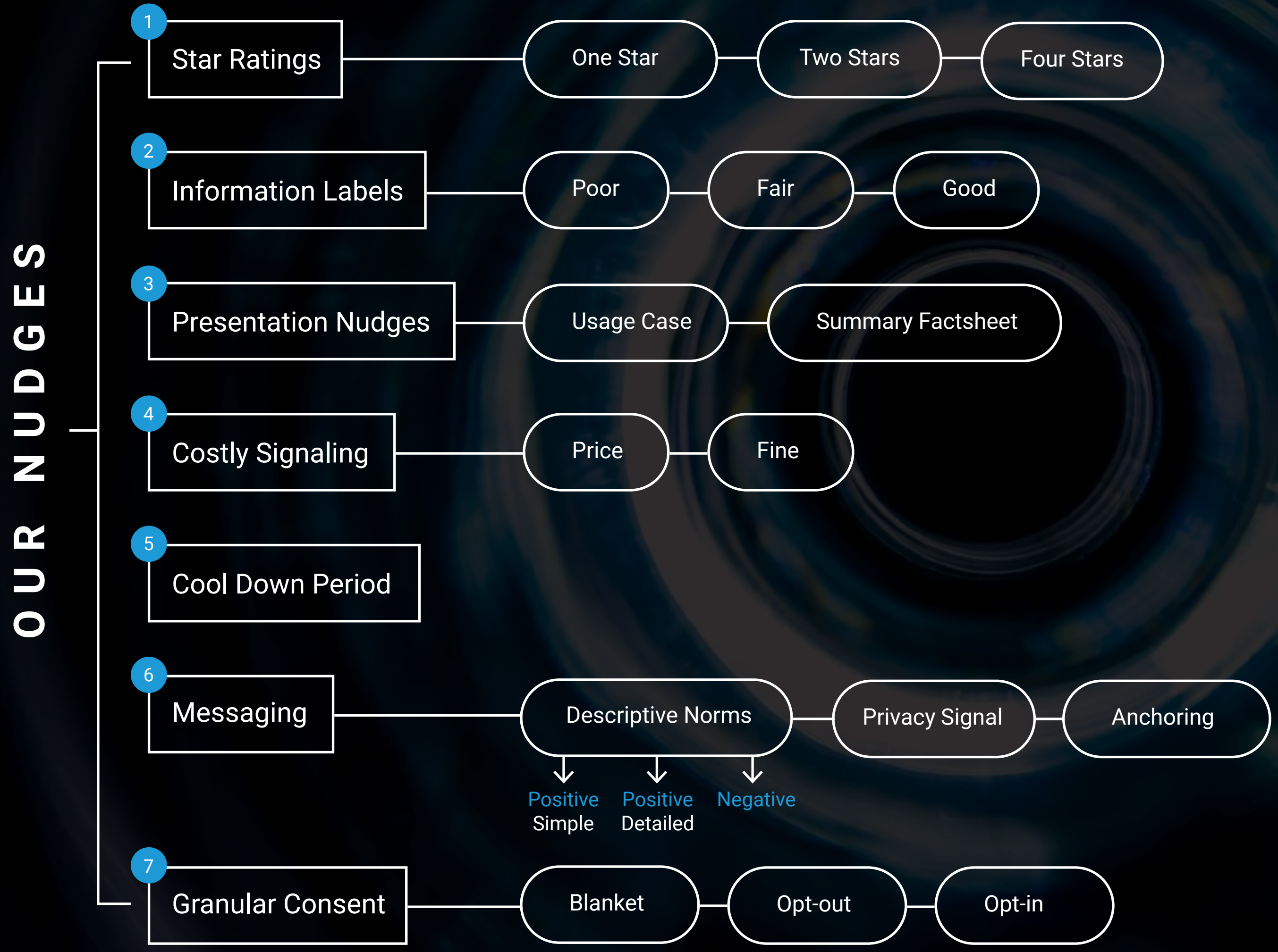


There are many biases at play, two of which are these:

Cognitive overload
Privacy statements are several pages long and full of complex legal jargon that prevent users from reading and understanding the policy.

Present bias
Users prefer instant access to the service or app as the harm from unmindful data sharing is in the future and intangible today.

OUR NUDGES



1 Star Ratings: One Star — Two Stars — Four Stars

2 Information Labels: Poor — Fair — Good

Information nudges that provide a snapshot indication of the quality of the privacy policy

3 Presentation Nudges: Usage Case — Summary Factsheet

They enhance the presentation of the privacy policy to make it more salient

4 Costly Signaling: Price — Fine

They provide financial 'guarantees' in case of data loss

5 Cool Down Period

It mandates a user to stay of the privacy policy page for a fixed period of time

6 Messaging: Descriptive Norms (Positive Simple, Positive Detailed, Negative) — Privacy Signal — Anchoring

They use principles of conformity with social norms, third party validation and a relatable anchor to influence privacy choices

7 Granular Consent: Blanket — Opt-out — Opt-in

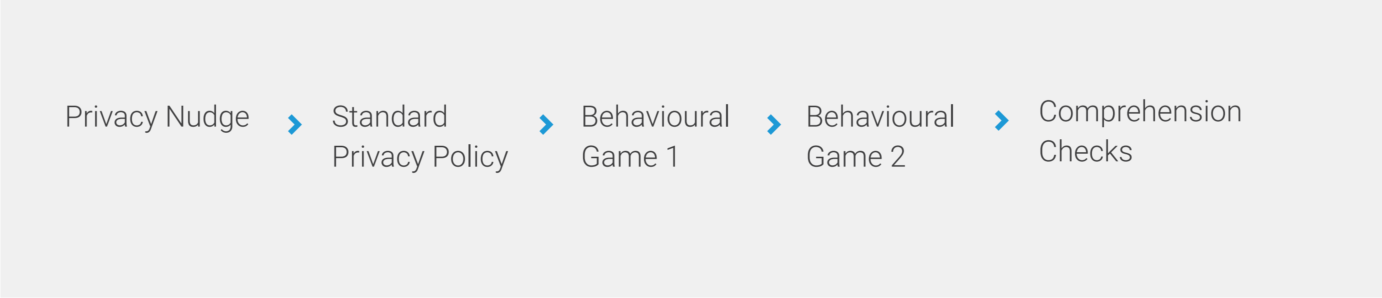
They provide granular breakup of the uses of data and an element of choice to the users

The Experiment Design

Participants from the experiment were divided into groups. Each group was shown a standard privacy statement along with one of the nudges; we compared these to a 'control group' that was only shown the privacy statement and no nudge.

All the groups were subsequently asked to play behavioural games followed by questions pertaining to the key points of the privacy policy to check their comprehension.

The responses were recorded and compared to understand the impact of each nudge vis-a-vis other nudges and the control group. We were measuring for four outcomes that are detailed in the next page.



Privacy Nudge › Standard Privacy Policy › Behavioural Game 1 › Behavioural Game 2 › Comprehension Checks

THE EXPERIMENTAL FACTSHEET

INDIA

No. of participants

5,547

KENYA

No. of participants

4,746

Participants Profiles

Males and females of average age of 28.5 years, mostly with at least bachelor's degree and average monthly income of over INR 20,000 in India and over KES 15,000 in Kenya

Medium

Online, using Qualtrics

4 Key Outcomes

Privacy means different things to different people. Is it how much of the users' personal information is available online, how the information is being used or who has access to this information? Everyone feels differently to varying degrees. As such we set out to make the users more cognizant of their own preferences and notions of privacy. This is what we call ***privacy consciousness***

We set out to measure impact on four key privacy-related behaviours.

Time spent on the privacy policy

We measured the amount of time (in seconds) spent by the users on the privacy page as it would indicate their effort to obtain privacy related information

Understanding of the policy terms

We asked a set of questions to measure recall and comprehension of key points from the privacy policy to reveal the quality of user engagement and whether they actually understood what they were consenting to.

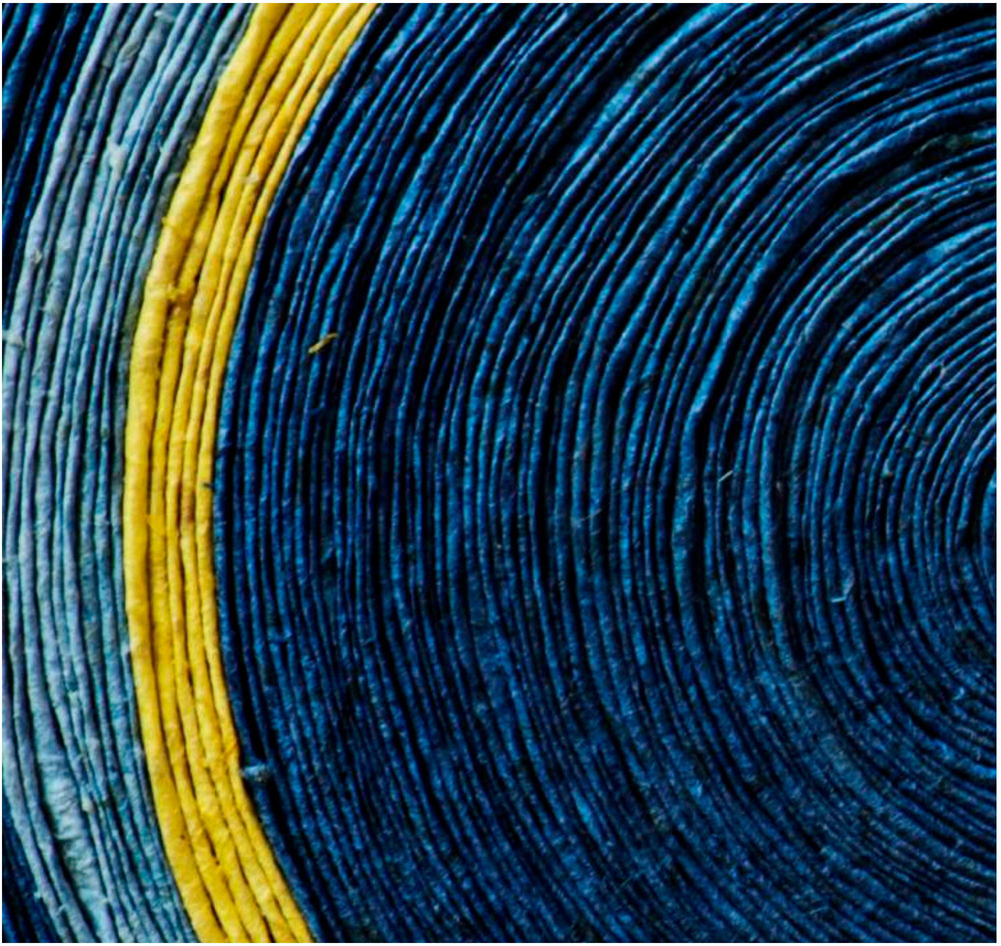
Sharing sensitive information

We asked users a set of invasive questions to be answered as Yes/ No to measure willingness to admit to behaviours, ranging from slightly sensitive to highly sensitive, like "Have you eaten meat, fish or poultry in the last year?" to "Have you had sexual relations with the current partner of a friend or family member?" We hypothesized that if the users trusted the entity asking the questions, they would be more willing to divulge responses to these questions.

Sharing personal information

We created a list of ten questions about the users' political beliefs, financial habits, and health, like "Which political party do you support?" and "Which medication do you take regularly?" We told participants that the purpose of this survey was to contact them with studies that they were interested in or cared about to see if there is more willingness to share information if users see benefits. If the users select 'Yes', that they would like to answer the question, they are then asked to type in their answer.

4 KEY OUTCOMES



Change in these behaviours due to exposure to our interventions revealed whether the users were successfully nudged to be more mindful of their privacy or not. We found that some of our interventions impacted trust of the users and thus their data sharing while others moved the needle on time spent or understanding of the policy. In some cases, data sharing reduced when privacy concerns were made salient. Some ideas had no significant impact on any of these outcomes. We also observed differences in responses of Indian and Kenyan participants for some nudges, signifying the role of context in how people behave. A brief snapshot of intervention - outcome impact mapping is presented in the next page.

	Time spent		Comprehension		Sharing sensitive information		Sharing personal information	
	INDIA	KENYA	INDIA	KENYA	INDIA	KENYA	INDIA	KENYA
Privacy Star Rating 1	🟥	🟥	🟥	🔴	🟩	🟩	🟥	🟥
Privacy Star Rating 2	🟥	🟥	🟢	🟥	🟩	🟥	🟩	🟥
Privacy Star Rating 4	🟥	🟥	🟩	🔴	🟩	🟢	🟩	🔴
Summary Factsheet	🟥	🟥	🟢	🟥	🟩	🟩	🟩	🔴
Usage Case	🟥	🔴	🟥	🟥	🟩	🟥	🟥	🔴
Costly Signal - Price	🟥	🟥	🟩	🟩	🟩	🟩	🟥	🔴
Costly Signal - Fine	🟥	🟥	🟩	🟥	🟩	🟩	🟩	🟥
Info-label - Below Average	🟥	🟥	🟩	🟥	🟩	🟥	🟥	🟥
Info-label- Average	🟥	🟥	🟩	🟥	🟩	🟩	🟩	🟥
Info-label - Above Average	🟥	🟥	🟩	🟩	🟩	🟩	🟩	🟥
Cool Down Period	N/A	N/A	🟢	🟢	🟢	🟩	🟢	🟩

Index

Positive Impact
(compared to results of the control group)

🟢 Significant

🟩 Not Significant

Negative Impact
(compared to results of the control group)

🔴 Significant

🟥 Not Significant

⬛ Opposite results in India and Kenya

	Time spent		Comprehension		Sharing sensitive information		Sharing personal information	
	INDIA	KENYA	INDIA	KENYA	INDIA	KENYA	INDIA	KENYA
Descriptive Norm - Simple	🟢	🟢	🟩	🟩	⚫ 🟩	⚫ 🟥	⚫ 🟥	⚫ 🟩
Descriptive Norm - Detailed	🟢	🟢	🟩	🟩	⚫ 🟩	⚫ 🟥	⚫ 🟥	⚫ 🟩
Descriptive Norm - Negative	🟢	🟢	🟩	🟢	⚫ 🟩	⚫ 🟥	⚫ 🟥	⚫ 🟩
Privacy Signal	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩
Anchoring	🟩	🟢	🟩	🟩	🟩	🟩	🟩	🟢
GC Blanket Consent	🟥	🟥	⚫ 🟥	⚫ 🟩	⚫ 🟥	⚫ 🟩	⚫ 🟥	⚫ 🟩
GC All Selected (Opt-out)	🟩	🟩	🟩	🟩	🟥	🟥	🟩	🟩
GC Essential Selected (Opt-In)	🟩	🟢	⚫ 🟥	⚫ 🟢	🟥	🟥	⚫ 🟥	⚫ 🟩

Index

Positive Impact
(compared to results of the control group)

🟢 Significant 🟩 Not Significant

Negative Impact
(compared to results of the control group)

🔴 Significant 🟥 Not Significant

⚫ Opposite results in India and Kenya

Key Findings from the Research

1 Comprehension of privacy policies is low, and is hard to nudge; further link between comprehension and user behaviour is weak

Nudging comprehension is not easy: In its current form, comprehension of standard privacy policy is low (not surprising). Even when results showed a significant increase in time spent on the privacy policy page, like in the case of positive descriptive norm nudging, it was not accompanied by an increase in comprehension of the policy terms. The cool down period nudge stood out in improving comprehension in both India and Kenya. In India, users' comprehension is surprisingly resilient to soft nudges; this is seen across multiple interventions. Negative norm nudging and the opt-in option for the granular consent nudge in Kenya impacted this outcome significantly.

Further, increasing comprehension of the privacy policy alone may not always lead to change in information sharing behaviour. In treatments like the summary factsheet, where comprehension has been nudged, willingness to share measures remain stubborn.

KEY FINDINGS

2

It is possible to nudge users' behaviour when it comes to data sharing - by increasing trust or by making privacy concerns salient

Data sharing can be increased by increasing trust

In India, the cool down period and the high star ratings nudges increased trust among users. The former worked by mandating them to stay on the policy page for a predetermined period of time, while users accepted the higher star rating as a viable indicator of better privacy practices. These perhaps indicated the platform was user centric and had nothing to hide.

Data sharing can be reduced by making privacy concerns salient, easiest way is to show 'how data is being used'

When users understood how their data would be used, they were more conscious of the privacy of their data. Usage case and blanket consent nudges, which laid out different uses of data in a more easy and comprehensible way, directionally reduced data sharing. In Kenya, nudges such as Summary Factsheet and Costly Price Signal also primed privacy concerns and worked similar to the usage case.

KEY FINDINGS

3

Default settings are critical; giving users more control less so

People don't change the default choice presented to them. 64% of respondents in India and 83% in Kenya accepted all the pre selected options in the granular consent nudge where they could opt out of the various data usage cases presented to them. This also proves that giving more control to users does not necessarily lead to them exercising it and hence has limited benefits.

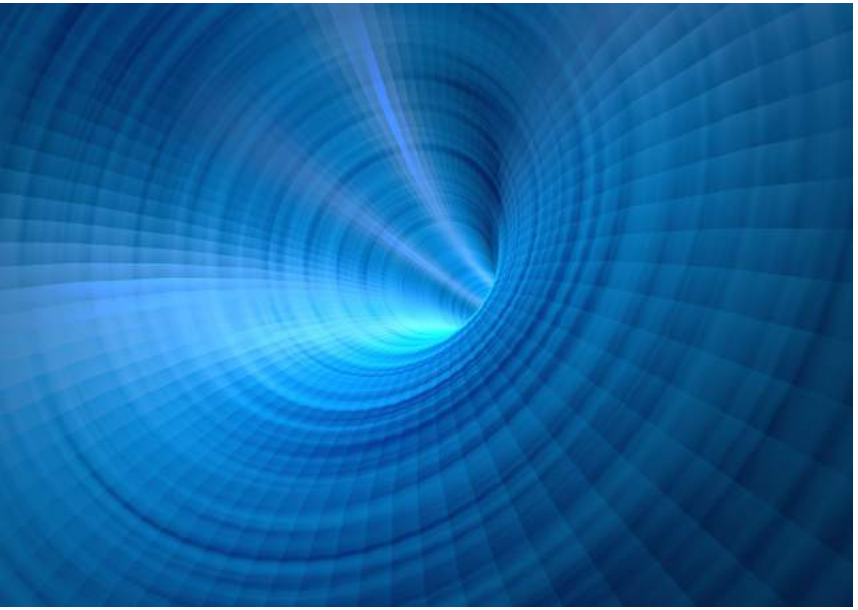
4

Most effective nudges are "hard" nudges that require integration into the product design

Different nudges have been successful in influencing user behaviour in different country contexts. In India, hard nudges, like the cool down period and defaults which shape the choice architecture and are integrated into the design, are more effective. On the other hand, 'soft', non-intrusive nudges like privacy signalling messages, the negative norm message and summary factsheet have worked well in Kenya.

Implications of Our Research

An overarching implication we have arrived at is that real impact in protecting the privacy interest of users can only be driven by **regulation**. Individuals are less capable and businesses are not-so incentivised to put privacy first.



Users need to be protected by regulators

It is hard for the users to take decisions in their best interest. Their privacy related behaviour is subjected to biases that are hard to overcome, like the high cognitive load they experience while going through the long and jargon filled privacy policy statement. Users can be nudged, but there aren't any easy fixes. For instance, improving comprehension or handing greater control to users seem to have limited impact on driving privacy conscious behaviours.

Businesses need a regulatory push to adopt better privacy practices

Nudges that have shown promise require design changes, like the cool down period or use of better default settings. It is unlikely for industry to formulate and adapt standards that could lead to business risk, like increasing friction in the user journey that can lead to higher drop outs or have defaults that lead to less data collection.

Some nudges have shown that better privacy features can increase trust and in some cases, even data sharing. Thus, it's a win-win for businesses and consumers. However, industry wide adoption of such practices would still require a regulatory push. For example, adopting a star rating framework is an increased cost for all players, as they would have to invest more to achieve and/ or maintain high ratings. It could also impact smaller players disproportionately.

Next Steps

Our experiments have opened the privacy landscape for further behavioural research through some compelling findings. We propose use of behavioural principles to further the better-privacy discourse.

Further experimentation

We must focus on further development of nudges that have shown promise, like the star ratings and cool down period and also explore the scope to combine treatments. Some of the specific areas that require deliberation are listed here.

Star ratings

What framework is used to generate these ratings? Who will be responsible to provide these ratings? How to ensure that this does not innately put a disproportionate burden on small players and give an unfair advantage to big players?

Cool down period

What is the optimal time period to balance user friction with improved comprehension? How to execute in real life? Could a shorter cool-down time combined with simplifying the policy work?

Defaults

What are the right default settings? Which privacy giving defaults need a statutory push? Meanwhile, regulators also need to keep an eye out for how defaults are being used in the industry since there is potential for overriding true user preference

NEXT STEPS

Live market tests

Working with service providers to test the adoption and applicability of the treatments in real market setting is a necessary step before any scale up plans.

Advocating ‘privacy by design’

Privacy should not be superimposed as an afterthought, but should be an important element or key parameter impacting the design and architecture of digital solutions. Thus, we recommend continued dialogue with service providers and regulators to adopt a more integrated approach to privacy and make consent part of the planned user experience.

THE BEHAVIOURAL EXPERIMENT

Why Privacy is a Behavioural Problem

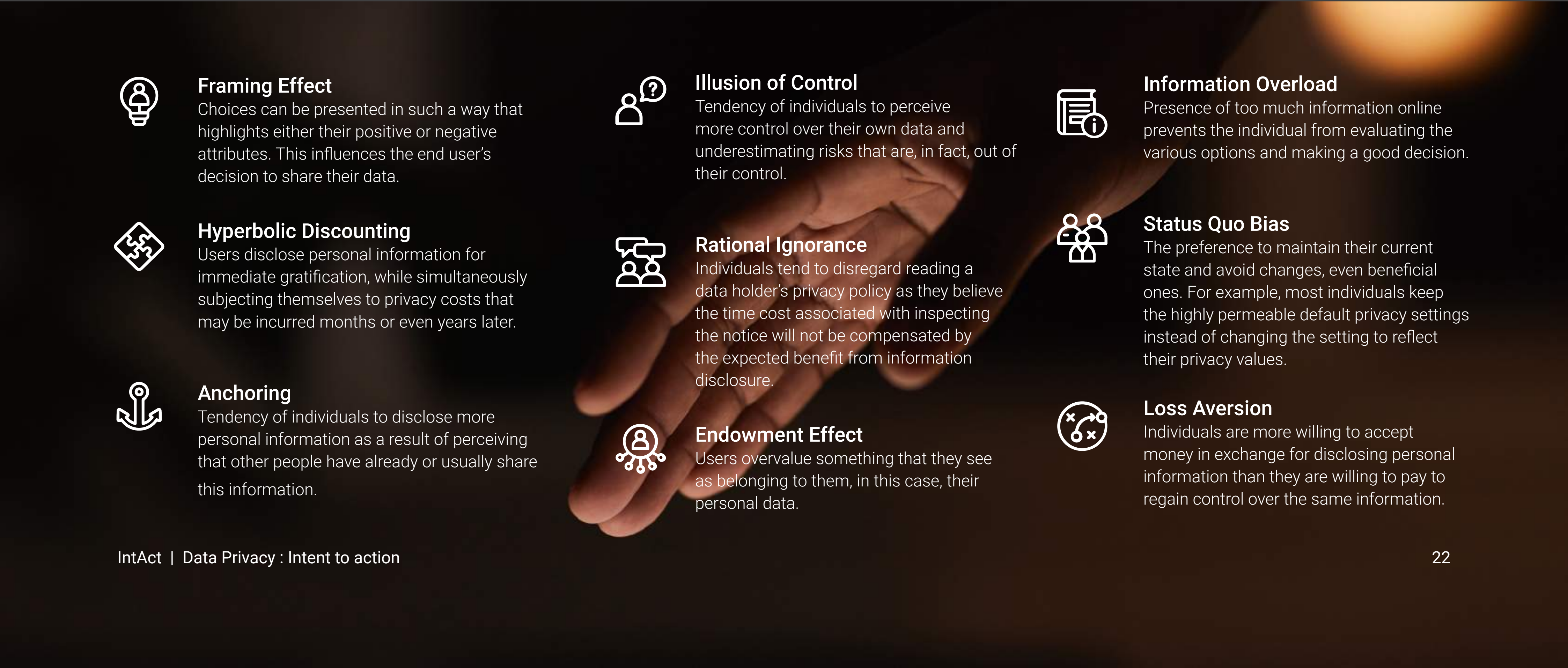
Many core issues in data privacy are primarily behavioural in nature. Consumers strongly prefer protecting their data, but when it comes to actually sharing their data, their resolution crumbles. Individuals feel a sense of ownership over their personal data, which makes them believe their data is more valuable than it actually might be. Users are often plagued by the "intention-action" gap, which can be seen by people wanting to protect their data but failing to do so due to distractions, competing priorities, or behavioural biases.

In addition to individuals facing behavioural barriers and inconsistencies in their own preferences, they are also subject to complex choice environments. Most apps have detailed policies at the beginning, which provide too much information in completely inaccessible ways. Privacy settings are often hidden away and need to be looked for. The notion of transparency between the user and business is compromised because businesses can benefit from collecting as much user data as possible.

Improving data privacy for users requires an understanding of human behaviour and how to design choices that help people make better decisions. Studying these barriers to good decisions will give businesses and regulators ideas about how they improve their own systems and foster a safer environment for users. At IntAct, we are using our understanding of people's behaviours to encourage them to be more privacy conscious while encouraging businesses to build trust, transparency, and loyalty for a longer and mutually beneficial engagement with their consumers. The first step was to understand the nuances of how people behave online and what traps they faced.

Behavioural Biases and Data Privacy

There is a growing body of research showing that our data privacy preferences may be prone to a number of behavioural biases. Here are some examples of how behavioural science concepts can explain how people make decisions online



Framing Effect

Choices can be presented in such a way that highlights either their positive or negative attributes. This influences the end user's decision to share their data.

Hyperbolic Discounting

Users disclose personal information for immediate gratification, while simultaneously subjecting themselves to privacy costs that may be incurred months or even years later.

Anchoring

Tendency of individuals to disclose more personal information as a result of perceiving that other people have already or usually share this information.

Illusion of Control

Tendency of individuals to perceive more control over their own data and underestimating risks that are, in fact, out of their control.

Rational Ignorance

Individuals tend to disregard reading a data holder's privacy policy as they believe the time cost associated with inspecting the notice will not be compensated by the expected benefit from information disclosure.

Endowment Effect

Users overvalue something that they see as belonging to them, in this case, their personal data.

Information Overload

Presence of too much information online prevents the individual from evaluating the various options and making a good decision.

Status Quo Bias

The preference to maintain their current state and avoid changes, even beneficial ones. For example, most individuals keep the highly permeable default privacy settings instead of changing the setting to reflect their privacy values.

Loss Aversion

Individuals are more willing to accept money in exchange for disclosing personal information than they are willing to pay to regain control over the same information.

OUR NUDGES

What are nudges

A nudge is the most common and handy tool in a behavioural scientist's toolbox. Nudges are interventions which are designed to remove behavioural biases and barriers in a decision-making scenario without changing the nature of the decision being made. A nudge often targets a specific bias and is non-intrusive in nature i.e. a decision maker can choose to ignore the nudge altogether.

What are some examples of nudges we see around us?

Text reminders to pay phone bills

Messages on social media that tell you who will be able to see photos or posts you're uploading

Your phone giving you a warning message when the battery drops to 20%

How our nudges target privacy decisions?

We carefully selected our nudges to target the most common behavioural biases that users face while making privacy related decisions. For example, presentation nudges target information overload and rational ignorance while cool down period targets present bias. In this section we map each of our nudges on to a relevant behavioural barrier/mechanisms

With an understanding of how people make decisions online, we developed and tested ideas which would help consumers to be more privacy conscious and show businesses that creating user-centric privacy practices could be an advantage.

At IntAct, we were especially interested in how people start using a new app or online service, so we focused on the consent process of the privacy policy, which is one of the first steps in a user's journey.

Privacy Star Ratings

What is the Nudge?

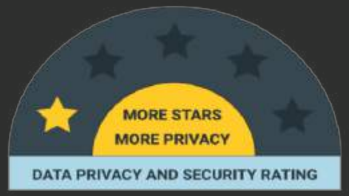
Users are given an **indication of the quality of privacy policy** through a star rating and are shown 1,2 or 4 star ratings. This treatment is inspired by electricity appliance ratings.

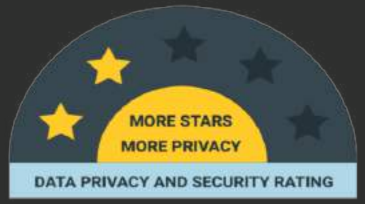
Behavioural underpinnings

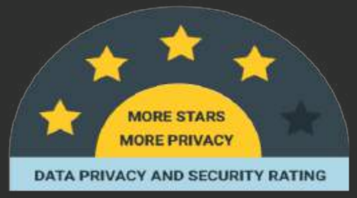
Ratings help users make a **quick judgement about the quality/ strength of a privacy policy** without having to go through the policy, circumventing common behavioural barriers like cognitive or information overload. This is likely to influence users' trust in the data collector

Hypothesis

We predicted that more stars will lead to greater information sharing







Information Label Ratings

What is the nudge?

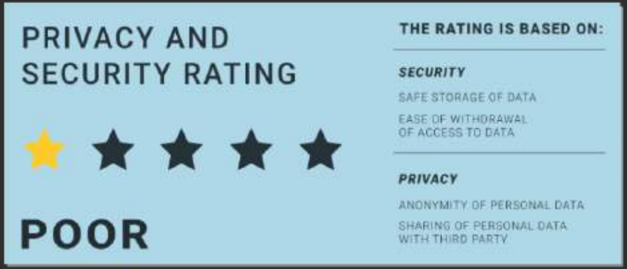
Users are given an **indication of quality of privacy policy** through a star rating along with some information, which explains the basis for the ratings. The inspiration comes from nutrition labels on food articles

Behavioural underpinnings

Ratings help users make a **quick judgement about the quality/ strength of a privacy policy** without having to go through the policy, circumventing common behavioural barriers like cognitive or information overload. This is likely to influences users' trust in the data collector

Hypothesis

We predicted that a better label (along with correspondingly higher stars) will lead to more information sharing



PRIVACY AND SECURITY RATING

POOR

THE RATING IS BASED ON:

SECURITY

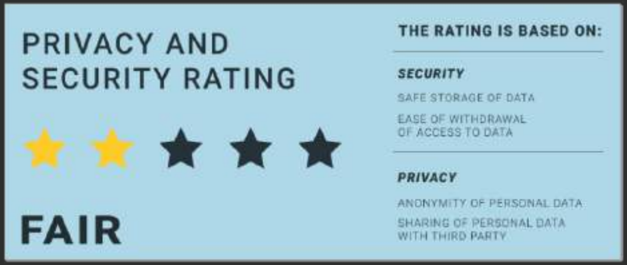
SAFE STORAGE OF DATA

EASE OF WITHDRAWAL OF ACCESS TO DATA

PRIVACY

ANONYMITY OF PERSONAL DATA

SHARING OF PERSONAL DATA WITH THIRD PARTY



PRIVACY AND SECURITY RATING

FAIR

THE RATING IS BASED ON:

SECURITY

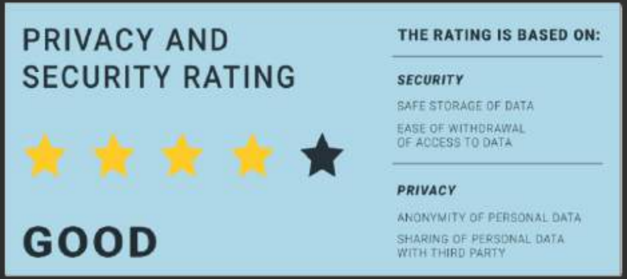
SAFE STORAGE OF DATA

EASE OF WITHDRAWAL OF ACCESS TO DATA

PRIVACY

ANONYMITY OF PERSONAL DATA

SHARING OF PERSONAL DATA WITH THIRD PARTY



PRIVACY AND SECURITY RATING

GOOD

THE RATING IS BASED ON:

SECURITY

SAFE STORAGE OF DATA

EASE OF WITHDRAWAL OF ACCESS TO DATA

PRIVACY

ANONYMITY OF PERSONAL DATA

SHARING OF PERSONAL DATA WITH THIRD PARTY

Summary Factsheet

What is the nudge?

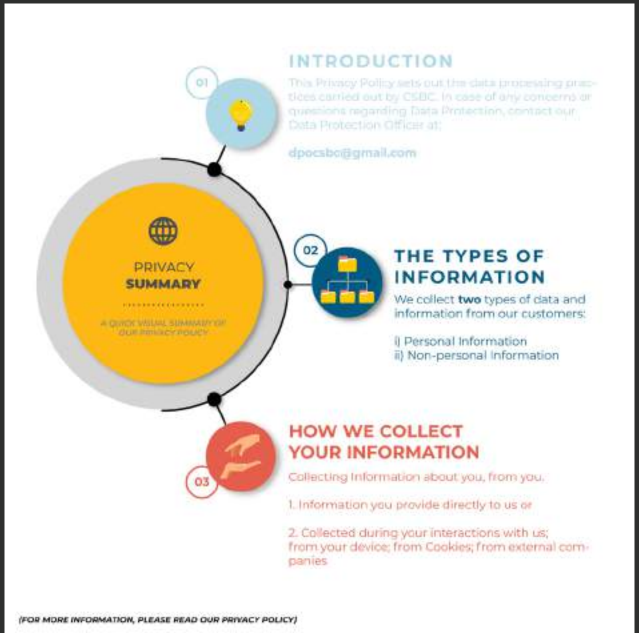
Presenting a **short summary of the privacy policy** using infographics to make the presentation appealing. The summary itself was made user friendly, jargon free and concise. We presented the ~2500 word policy as a less than 500 word summary

Behavioural underpinnings

The summary factsheet simplifies the privacy policy and **avoids behavioural impediments like cognitive overload**, allowing users to make an informed choice about their decision. Better understanding of policy can lead to more trust and information sharing

Hypothesis

We predicted that the summary factsheet will lead to more information sharing and improved policy comprehension



PRIVACY **SUMMARY**

A QUICK VISUAL SUMMARY OF OUR PRIVACY POLICY

01 INTRODUCTION

This Privacy Policy sets out the data processing practices carried out by CSBC. In case of any concerns or questions regarding Data Protection, contact our Data Protection Officer at:

dpocsbc@gmail.com

02 THE TYPES OF INFORMATION

We collect **two** types of data and information from our customers:

i) Personal Information
ii) Non-personal Information

03 HOW WE COLLECT YOUR INFORMATION

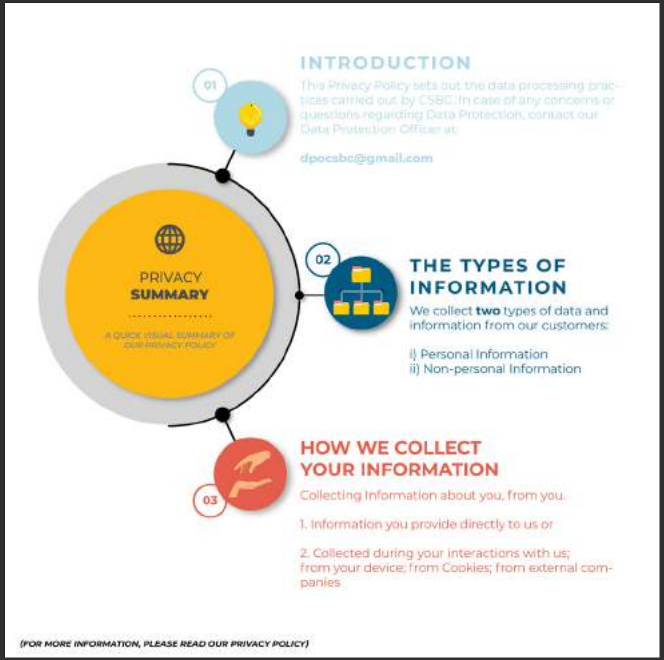
Collecting Information about you, from you.

1. Information you provide directly to us or

2. Collected during your interactions with us; from your device; from Cookies; from external companies

(FOR MORE INFORMATION, PLEASE READ OUR PRIVACY POLICY)

> Summary Factsheet



PRIVACY **SUMMARY**

A QUICK VISUAL SUMMARY OF OUR PRIVACY POLICY

01

INTRODUCTION

This Privacy Policy sets out the data processing practices carried out by CSBC. In case of any concerns or questions regarding Data Protection, contact our Data Protection Officer at:

dpocsbc@gmail.com

02

THE TYPES OF INFORMATION

We collect **two** types of data and information from our customers:

i) Personal Information
ii) Non-personal Information

03

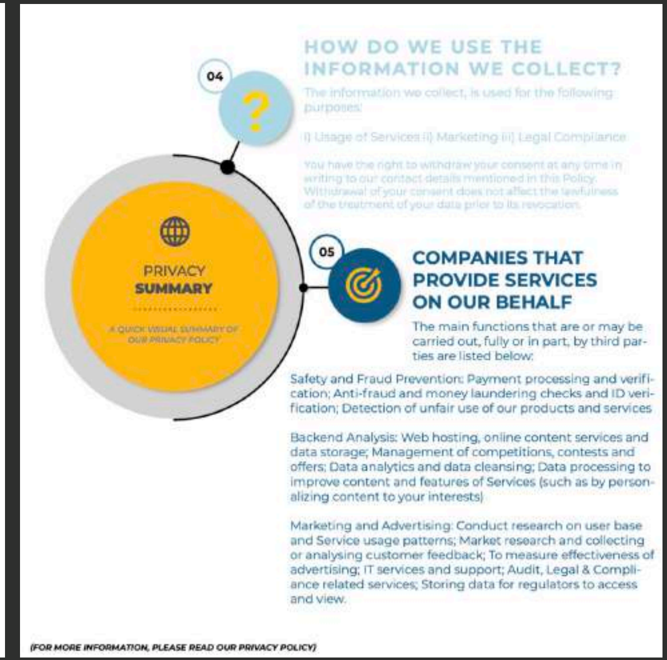
HOW WE COLLECT YOUR INFORMATION

Collecting Information about you, from you.

1. Information you provide directly to us or

2. Collected during your interactions with us; from your device; from Cookies; from external companies

(FOR MORE INFORMATION, PLEASE READ OUR PRIVACY POLICY)



PRIVACY **SUMMARY**

A QUICK VISUAL SUMMARY OF OUR PRIVACY POLICY

04

HOW DO WE USE THE INFORMATION WE COLLECT?

The information we collect, is used for the following purposes:

i) Usage of Services ii) Marketing iii) Legal Compliance

You have the right to withdraw your consent at any time in writing to our contact details mentioned in this Policy. Withdrawal of your consent does not affect the lawfulness of the treatment of your data prior to its revocation.

05

COMPANIES THAT PROVIDE SERVICES ON OUR BEHALF

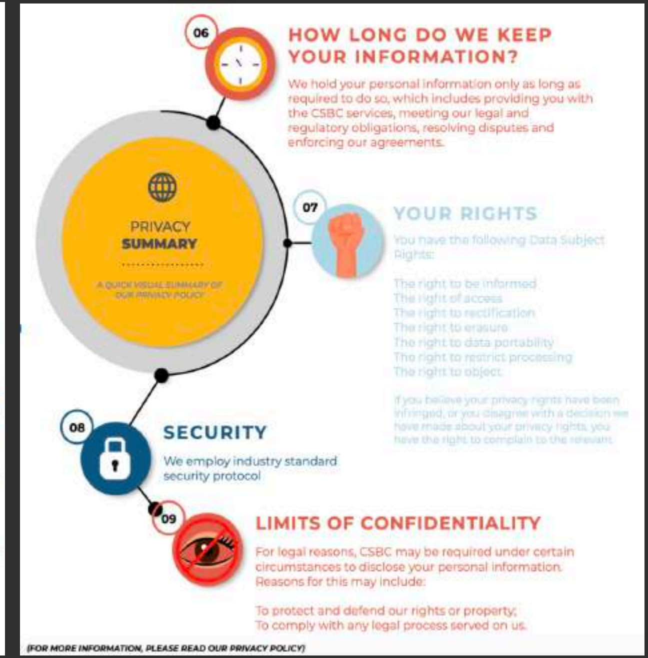
The main functions that are or may be carried out, fully or in part, by third parties are listed below:

Safety and Fraud Prevention: Payment processing and verification; Anti-fraud and money laundering checks and ID verification; Detection of unfair use of our products and services

Backend Analysis: Web hosting, online content services and data storage; Management of competitions, contests and offers; Data analytics and data cleansing; Data processing to improve content and features of Services (such as by personalizing content to your interests)

Marketing and Advertising: Conduct research on user base and Service usage patterns; Market research and collecting or analysing customer feedback; To measure effectiveness of advertising; IT services and support; Audit, Legal & Compliance related services; Storing data for regulators to access and view.

(FOR MORE INFORMATION, PLEASE READ OUR PRIVACY POLICY)



PRIVACY **SUMMARY**

A QUICK VISUAL SUMMARY OF OUR PRIVACY POLICY

06

HOW LONG DO WE KEEP YOUR INFORMATION?

We hold your personal information only as long as required to do so, which includes providing you with the CSBC services, meeting our legal and regulatory obligations, resolving disputes and enforcing our agreements.

07

YOUR RIGHTS

You have the following Data Subject Rights:

The right to be informed
The right of access
The right to rectification
The right to erasure
The right to data portability
The right to restrict processing
The right to object

If you believe your privacy rights have been infringed, or you disagree with a decision we have made about your privacy rights, you have the right to complain to the relevant

08

SECURITY

We employ industry standard security protocol

09

LIMITS OF CONFIDENTIALITY

For legal reasons, CSBC may be required under certain circumstances to disclose your personal information. Reasons for this may include:

To protect and defend our rights or property;
To comply with any legal process served on us.

(FOR MORE INFORMATION, PLEASE READ OUR PRIVACY POLICY)

Usage Case

What is the nudge?

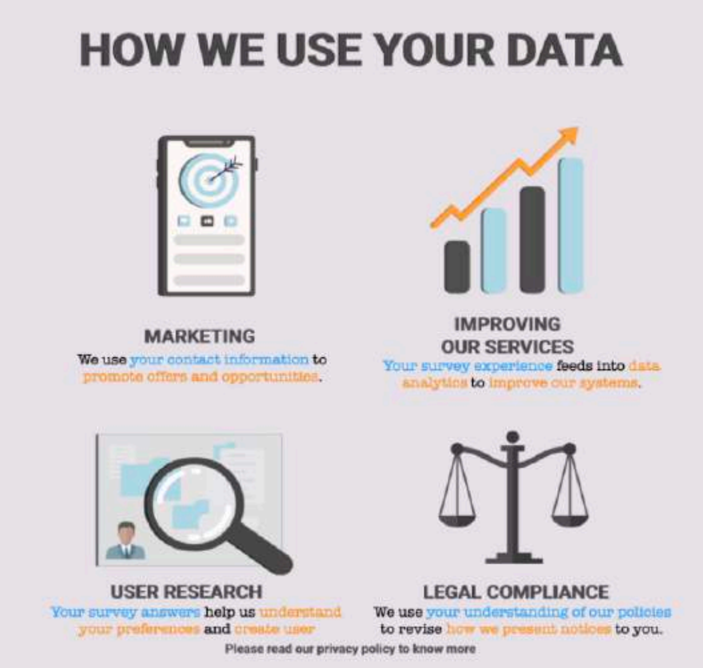
An infographic showing how **user information will be utilised**. It is important to users to know how collected data is used while making decisions about sharing their data. Simple icons and language which can easily be understood by all users

Behavioural underpinnings

Sharing information on data use with users can **address the problem of information asymmetry** (that businesses know more about how data is used than users) and improve user trust in data sharing

Hypothesis

We predicted that presenting the usage case will lead to more information sharing as businesses are more up front about how they use data



HOW WE USE YOUR DATA

MARKETING

We use your contact information to promote offers and opportunities.

IMPROVING OUR SERVICES

Your survey experience feeds into data analytics to improve our systems.

USER RESEARCH

Your survey answers help us understand your preferences and create user

LEGAL COMPLIANCE

We use your understanding of our policies to revise how we present notices to you.

Please read our privacy policy to know more

Costly Signal

What is the nudge?

We tested two costly signals:

- *A price signal where users will be paid a certain amount as compensation in case of a breach*
- *A fine signal where the company will be subjected to a fine by the government in case of a breach*

Behavioural underpinnings

Costly signal works like a traditional **guarantee to influence user trust** in sharing information. It provides users with a risk mitigating option against the risk of losing their data or its unauthorised use

Hypothesis

We predicted that costly signal will lead to more information sharing

Any data shared with Busara is protected with the strongest available security measures.

Incase of any breach, you will be compensated with $10,000

Any data shared with Busara is protected with the strongest available security measures.

Incase of any data breach, the company will pay the government a fine stipulated by Data Protection Law

Cool Down Period

What is the nudge?

Users are made to stay on the privacy policy page for a few minutes (6 minutes in this case) before moving ahead. The aim was to ensure they read through the policy to have a better understanding of its terms

Behavioural underpinnings

By mandating users to stay on the privacy policy for a stipulated period of time, **a cool down period mitigates the present bias** - where the users agree to the policy solely to gain immediate access to the desired product or service without duly considering personal cost of sharing data

Hypothesis

We predicted that cool down period will lead to more information sharing and better policy comprehension

Positive Descriptive Norms

What is the nudge?

Users are shown a normative message just before reading the privacy policy. The message nudges users to spend a specific amount of time in reading the privacy policy. Positive norms show the prevalence and benefits of engaging in the recommended behaviour

Behavioural underpinnings

Conformity with social norms is a key motivator of human behaviour. It has been seen in previous literature that normative messaging can be used to **influence perceived and descriptive norms** which can lead to behaviour change

Hypothesis

We predicted that positive descriptive norms will lead to more time spent on policy and better policy comprehension

Over **70% of users** spend 5 minutes to read and understand our privacy policy

According to our research on users who took this survey before you, those who spend around 5 minutes reading our policy report higher comprehension scores and are able to make informed privacy decisions

Negative Descriptive Norms

What is the nudge?

Users are shown a normative message just before reading the privacy policy. The message nudges users to spend a specific amount of time in reading the privacy policy. Negative norms show the prevalence and risks of not engaging in the recommended behaviour

Behavioural underpinnings

Conformity with social norms is a key motivator of human behaviour. It has been seen in previous literature that normative messaging can be used to **influence perceived and descriptive norms** which can lead to behaviour change

Hypothesis

We predicted that negative descriptive norms will lead to more time spent on policy and better policy comprehension

89% of internet users **do not read** privacy policies before agreeing to share data, exposing themsleves to **avoidable risk**. Please **do not skip** this privacy policy.

Privacy Signal

What is the nudge?

Users read a message showing adherence to standard privacy principles like the GDPR framework. The aim is to use objective, verifiable statements as signalling device to communicate the data collector’s commitment towards data privacy

Behavioural underpinnings

Using standardised privacy frameworks which give an objective third-party validation to the data collector’s intentions to keep user data safe can **prime users to trust the data collector and that their data is safe**. This can make them comfortable in sharing more information

Hypothesis

We predicted that privacy signal will lead to more information sharing

We have appointed a **Data Protection Officer** as stipulated under the GDPR (an internationally recognized legal framework for privacy) to **address any of your concerns**. You can reach them at **info@intactprivacy.com**

Anchoring

What is the nudge?

Users are shown a message relating the recommended time spent on the privacy policy with an everyday task, say brushing their teeth. This gives them a relatable estimate on how long they should spend on the privacy policy to reap benefits

Behavioural underpinnings

The **length of the privacy policy can pose a cognitive barrier** for users who might give up on reading the policy. Relating this to a common use case for time spent can overcome this barrier by making the task of reading the policy appear less challenging and time consuming

Hypothesis

We predicted that anchoring will lead to more time spent on privacy policy and better policy comprehension

It takes **only 5 minutes to brush your teeth** everyday, the same amount of time as reading this policy and **making informed decisions**

Granular Blanket Consent

What is the nudge?

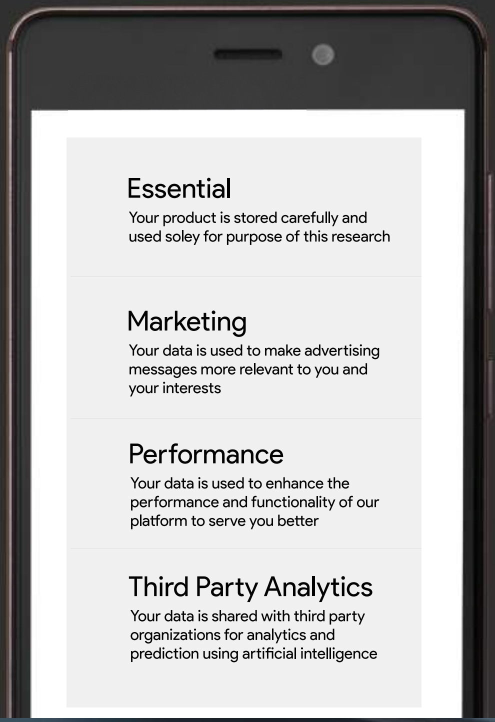
Users are shown a **granular breakup of how their data is used**, similar to cookie policy declarations on websites. Under the blanket consent, they can only say “Yes to All” or “No to All”.

Behavioural underpinnings

Showing users how their data is used and giving them an element of choice over this can make users comfortable in sharing more information by improving their **self-efficacy towards data-sharing decisions**

Hypothesis

We predicted that granular blanket consent will lead to more information sharing by users



Essential

Your product is stored carefully and used soley for purpose of this research

Marketing

Your data is used to make advertising messages more relevant to you and your interests

Performance

Your data is used to enhance the performance and functionality of our platform to serve you better

Third Party Analytics

Your data is shared with third party organizations for analytics and prediction using artificial intelligence

Granular Consent - Opt-out

What is the nudge?

Users are shown a granular breakup of how their data is used, similar to cookie policy declarations on websites. Under the in-out consent, users can choose any or all options with all options selected as the default.

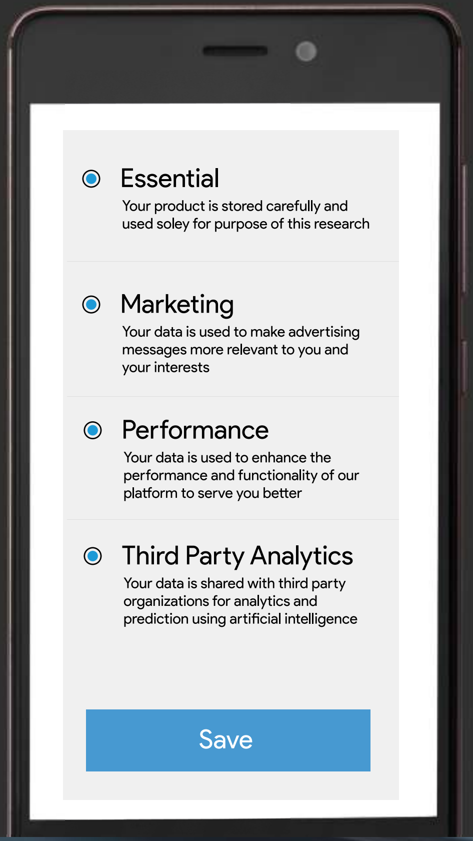
Behavioural underpinnings

Showing users how their data is used and giving them an element of choice over this can make users comfortable in sharing more information by improving their **self-efficacy towards data-sharing decisions**

Hypothesis

We predicted that granular consent will lead to more information sharing by users

We expected users to consent to data collection for more purposes in the opt-out default as compared to the opt-in default



◉ Essential

Your product is stored carefully and used soley for purpose of this research

◉ Marketing

Your data is used to make advertising messages more relevant to you and your interests

◉ Performance

Your data is used to enhance the performance and functionality of our platform to serve you better

◉ Third Party Analytics

Your data is shared with third party organizations for analytics and prediction using artificial intelligence

Granular Consent - Opt-in

What is the nudge?

Users are shown a **granular breakup of how their data is used**, similar to cookie policy declarations on websites. Under the opt-out consent, users can choose any or all options with only the essential option selected as the default.

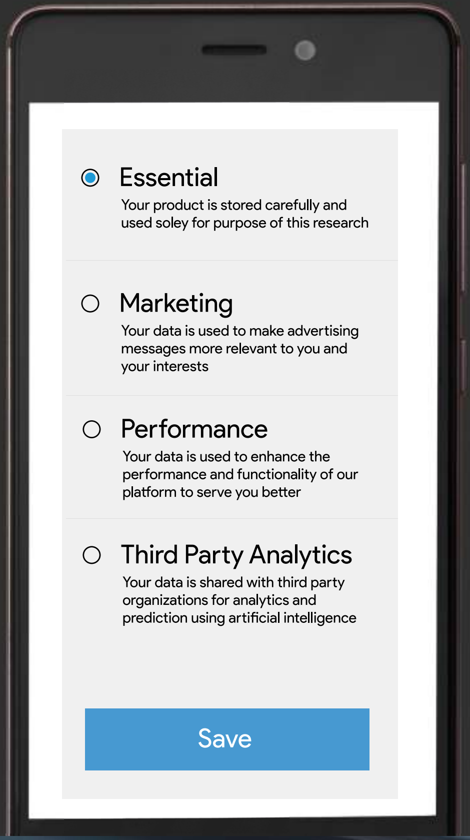
Behavioural underpinnings

Showing users how their data is used and giving them an element of choice over this can make users comfortable in sharing more information by improving their **self-efficacy towards data-sharing decisions**

Hypothesis

We predicted that granular consent will lead to more information sharing by users

We expected users to consent to data collection for more purposes in the opt-out default as compared to the opt-in default



● Essential
Your product is stored carefully and used soley for purpose of this research

○ Marketing
Your data is used to make advertising messages more relevant to you and your interests

○ Performance
Your data is used to enhance the performance and functionality of our platform to serve you better

○ Third Party Analytics
Your data is shared with third party organizations for analytics and prediction using artificial intelligence

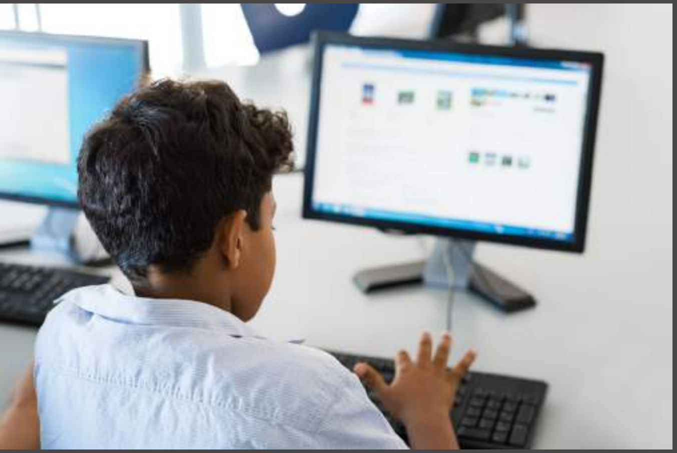
Experiment Design

After designing our privacy nudges, we needed to check if they worked, which we did using an experiment. Our experiment had three main parts:

1 Privacy policy

2 Interventions to make individuals more privacy conscious

3 Questions that help us understand if our interventions are working



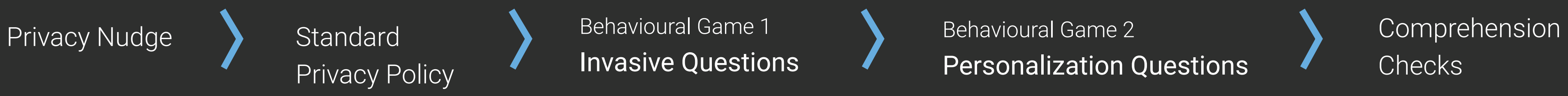
The privacy policy looked much like any other privacy policy. Our interventions or nudges were designed to accompany the privacy policy. Some interventions captured the same information as the privacy policy but in a more succinct way, while others encouraged people to spend some time going through the privacy policy.

To see how well the interventions were working, we needed to measure if people became more privacy conscious. Privacy consciousness meant that users started acting in line with their preferences, knew more about the privacy standards of the apps and online platforms they were using, and thought about sharing information. To test their understanding and recall of the privacy standards, individuals were asked to answer comprehension questions about the privacy policy. We also tracked how long they spent on the policy. To understand how the interventions affected how much information they shared, we asked respondents a series of invasive and personal questions.

Each individual went through the three different parts of our experiment. Once we had a number of respondents, we could start drawing conclusions about which interventions were working and which were not.

Experiment Flow

Around 5547 respondents in India and 4746 respondents in Kenya answered our survey online. As they began the experiment, they were randomly assigned into different groups, each of which received a different nudge. Respondents were first shown the standard privacy policy and one of the nudges. One of the groups was the ‘control’ group that was shown only the privacy policy and no nudge. Everyone, regardless of the intervention they received, then answered different sets of questions.



Privacy Nudge

Standard Privacy Policy

Behavioural Game 1
Invasive Questions

Behavioural Game 2
Personalization Questions

Comprehension Checks

WHO ANSWERED OUR SURVEY

INDIA

No. of Interviews

5,547

% Female

38%

Average Age (Range)

30

Years (18-60)

Education Levels

Primary and Lower: 2%
Secondary: 14%
Bachelors: 29%
Masters: 39%
Certificate / Diploma: 16%

Monthly Income

Less than Rs. 20,000: 42%
Rs. 20,000 - Rs. 80,000: 40%
Greater than Rs. 80,000: 18%

KENYA

No. of Interviews

4,746

% Female

58%

Average Age (Range)

27

Years (18-55)

Education Levels

Primary and Lower: 0.2%,
Secondary: 14%,
Bachelors: 47%,
Masters: 4%,
College/Vocational: 33%

Monthly Income

Less than KES 3,000: 29%,
KES 3,000-KES 15,000: 23%,
Greater than KES 15,000: 48%

MEASURING PRIVACY

Outcome Variables

We measured how users responded to our interventions by measuring behaviour across four outcome variables.

1

Time spent on privacy policy

Time spent, in seconds, on the privacy policy page to measure effort expended to obtain privacy related information

2

Comprehension

Set of questions to measure recall and comprehension of key points from the privacy policy

3

Willingness to share sensitive information

Set of invasive questions to be answered as Yes/No to measure willingness to admit to behaviours, ranging from slightly sensitive to highly sensitive

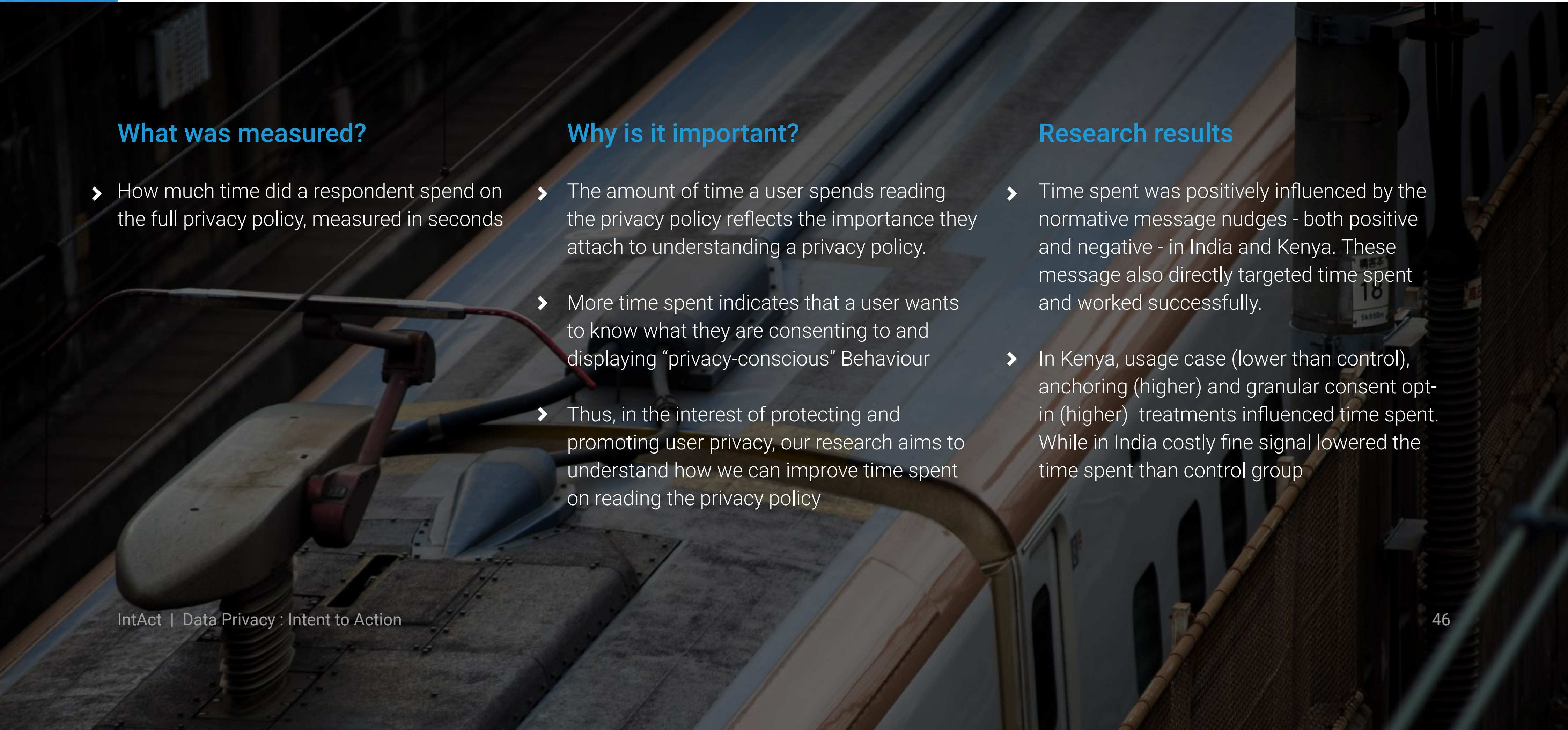
4

Willingness to share personal information

Set of questions which mimic an online service provider survey to improve service by asking for personal preferences and information

OUTCOME VARIABLES

1 Time spent on privacy policy



What was measured?

- How much time did a respondent spend on the full privacy policy, measured in seconds

Why is it important?

- The amount of time a user spends reading the privacy policy reflects the importance they attach to understanding a privacy policy.
- More time spent indicates that a user wants to know what they are consenting to and displaying “privacy-conscious” Behaviour
- Thus, in the interest of protecting and promoting user privacy, our research aims to understand how we can improve time spent on reading the privacy policy

Research results

- Time spent was positively influenced by the normative message nudges - both positive and negative - in India and Kenya. These message also directly targeted time spent and worked successfully.
- In Kenya, usage case (lower than control), anchoring (higher) and granular consent opt-in (higher) treatments influenced time spent. While in India costly fine signal lowered the time spent than control group

Time spent (in seconds) - Treatment vs. Control

TREATMENT	INDIA	KENYA
Control	29	147
Privacy Rating 1 Star	24	85
Privacy Rating 2 Star	25	90
Privacy Rating 4 Star	27	72
Summary Factsheet	27	63
Usage	23	57*
Costly Signal - Price	28	98
Costly Signal - Fine	21*	67
Info-label Combo - Below Average	27	61
Info-label Combo - Average	27	68
Info-label Combo - Above Average	26	77

Cool Down Period

Statistically significant:

**** at the 1% level ** at the 5% level * at the 10% level*

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

Time spent (in seconds) - Treatment vs. Control

TREATMENT	INDIA	KENYA
Control	20	55
Descriptive Norm - Simple	38***	86***
Descriptive Norm - Detailed	46***	110***
Descriptive Norm - Negative	31*	95***
Privacy Signal	21	62
Anchoring	25	73*
GC Blanket Consent	18	44
GC All Selected (Opt-out)	21	65
GC Essential Selected (Opt-in)	22	78**

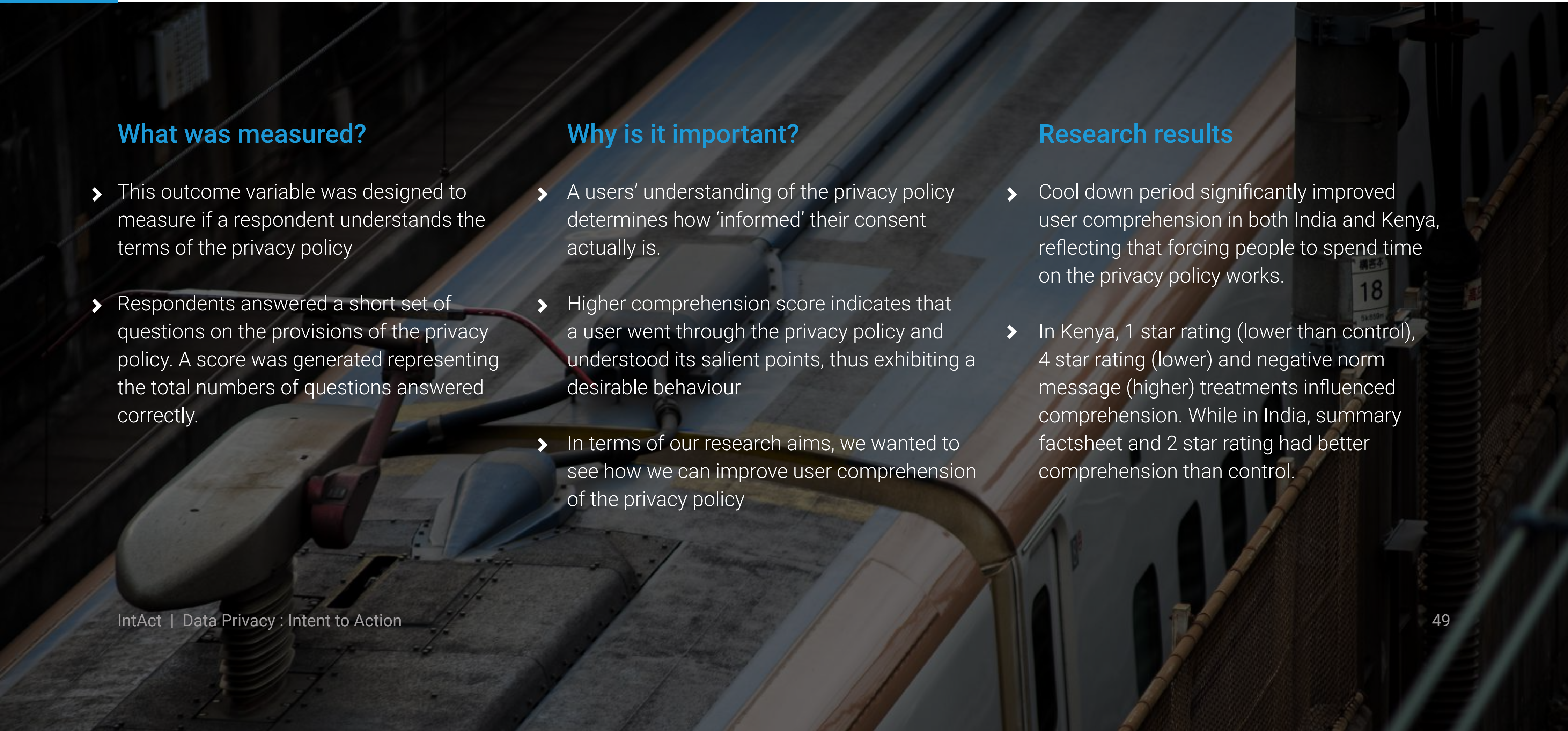
Statistically significant:
*** *at the 1% level* ** *at the 5% level* * *at the 10% level*

GC - Granular Consent

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

OUTCOME VARIABLES

2 Policy comprehension



What was measured?

- This outcome variable was designed to measure if a respondent understands the terms of the privacy policy
- Respondents answered a short set of questions on the provisions of the privacy policy. A score was generated representing the total numbers of questions answered correctly.

Why is it important?

- A users' understanding of the privacy policy determines how 'informed' their consent actually is.
- Higher comprehension score indicates that a user went through the privacy policy and understood its salient points, thus exhibiting a desirable behaviour
- In terms of our research aims, we wanted to see how we can improve user comprehension of the privacy policy

Research results

- Cool down period significantly improved user comprehension in both India and Kenya, reflecting that forcing people to spend time on the privacy policy works.
- In Kenya, 1 star rating (lower than control), 4 star rating (lower) and negative norm message (higher) treatments influenced comprehension. While in India, summary factsheet and 2 star rating had better comprehension than control.

Comprehension score - Treatment vs. Control

TREATMENT	INDIA	KENYA
Control	2.0	3.0
Privacy Rating 1 Star	2.0	2.7*
Privacy Rating 2 Star	2.2*	2.9
Privacy Rating 4 Star	2.1	2.7*
Summary Factsheet	2.2*	2.9
Usage	1.9	2.7
Costly Signal - Price	2.0	3.0
Costly Signal - Fine	2.1	2.8
Info-label Combo - Below Average	2.0	2.9
Info-label Combo - Average	2.1	2.9
Info-label Combo - Above Average	2.0	3.1
Cool Down Period	2.6***	3.8***

Statistically significant:

*** *at the 1% level* ** *at the 5% level* * *at the 10% level*

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

Comprehension score - Treatment vs. Control

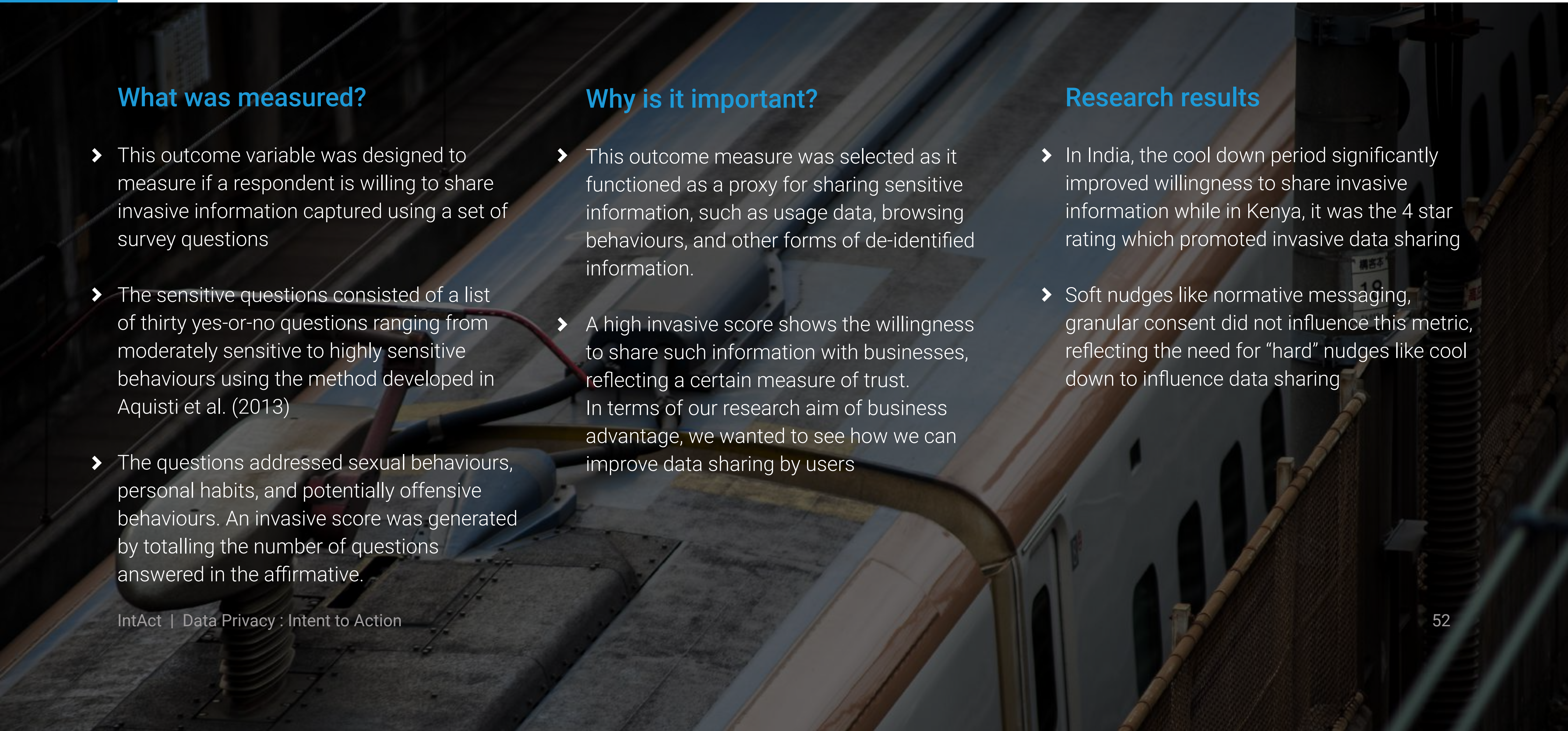
TREATMENT	INDIA	KENYA
Control	2.04	2.75
Descriptive Norm - Simple	2.12	2.80
Descriptive Norm - Detailed	2.18	2.86
Descriptive Norm - Negative	2.17	3.04**
Privacy Signal	2.24	2.93
Anchoring	2.19	2.84
GC Blanket Consent	1.98	2.82
GC All Selected (Opt-out)	2.15	2.90
GC Essential Selected (Opt-in)	2.02	3.05**

Statistically significant:

*** *at the 1% level* ** *at the 5% level* * *at the 10% level*

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

3 Willingness to share sensitive information



What was measured?

- This outcome variable was designed to measure if a respondent is willing to share invasive information captured using a set of survey questions
- The sensitive questions consisted of a list of thirty yes-or-no questions ranging from moderately sensitive to highly sensitive behaviours using the method developed in Aquisti et al. (2013)
- The questions addressed sexual behaviours, personal habits, and potentially offensive behaviours. An invasive score was generated by totalling the number of questions answered in the affirmative.

Why is it important?

- This outcome measure was selected as it functioned as a proxy for sharing sensitive information, such as usage data, browsing behaviours, and other forms of de-identified information.
- A high invasive score shows the willingness to share such information with businesses, reflecting a certain measure of trust. In terms of our research aim of business advantage, we wanted to see how we can improve data sharing by users

Research results

- In India, the cool down period significantly improved willingness to share invasive information while in Kenya, it was the 4 star rating which promoted invasive data sharing
- Soft nudges like normative messaging, granular consent did not influence this metric, reflecting the need for “hard” nudges like cool down to influence data sharing

Willingness to share sensitive information (sensitive score) - Treatment vs. Control

TREATMENT	INDIA	KENYA
Control	12.8	15.0
Privacy Rating 1 Star	13.0	15.6
Privacy Rating 2 Star	13.7	15.0
Privacy Rating 4 Star	13.7	15.8*
Summary Factsheet	13.6	15.0
Usage	13.8	14.8
Costly Signal - Price	13.7	15.2
Costly Signal - Fine	13.8	15.1
Info-label Combo - Below Average	13.4	14.9
Info-label Combo - Average	13.6	15.2
Info-label Combo - Above Average	13.4	15.3
Cool Down Period	14.9**	15.6

Statistically significant:

*** *at the 1% level* ** *at the 5% level* * *at the 10% level*

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

Willingness to share sensitive information (sensitive score) - Treatment vs. Control

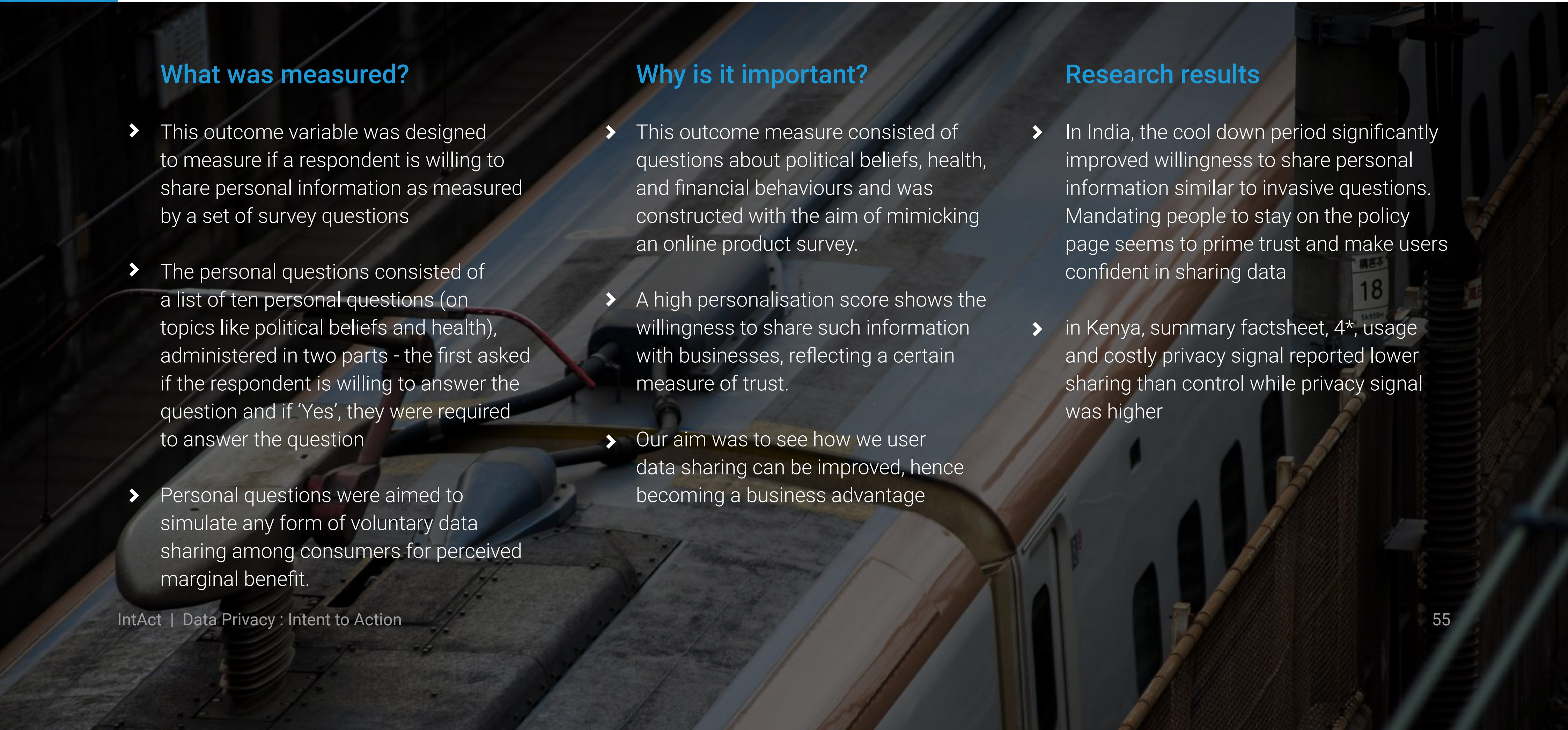
TREATMENT	INDIA	KENYA
Control	11.8	14.3
Descriptive Norm - Simple	12.4	13.5
Descriptive Norm - Detailed	12.0	14.0
Descriptive Norm - Negative	12.2	14.0
Privacy Signal	11.4	13.8
Anchoring	11.8	14.7
GC Blanket Consent	10.9	14.4
GC All Selected (Opt-out)	11.5	13.7
GC Essential Selected (Opt-in)	11.3	14.2

Statistically significant:
**** at the 1% level ** at the 5% level * at the 10% level*

GC - Granular Consent

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

4 Willingness to share personal information



What was measured?

- This outcome variable was designed to measure if a respondent is willing to share personal information as measured by a set of survey questions
- The personal questions consisted of a list of ten personal questions (on topics like political beliefs and health), administered in two parts - the first asked if the respondent is willing to answer the question and if 'Yes', they were required to answer the question
- Personal questions were aimed to simulate any form of voluntary data sharing among consumers for perceived marginal benefit.

Why is it important?

- This outcome measure consisted of questions about political beliefs, health, and financial behaviours and was constructed with the aim of mimicking an online product survey.
- A high personalisation score shows the willingness to share such information with businesses, reflecting a certain measure of trust.
- Our aim was to see how we user data sharing can be improved, hence becoming a business advantage

Research results

- In India, the cool down period significantly improved willingness to share personal information similar to invasive questions. Mandating people to stay on the policy page seems to prime trust and make users confident in sharing data
- in Kenya, summary factsheet, 4*, usage and costly privacy signal reported lower sharing than control while privacy signal was higher

Willingness to share personal information (personalisation score) - Treatment vs. Control

TREATMENT	INDIA	KENYA
Control	5.9	7.9
Privacy Rating 1 Star	5.8	7.5
Privacy Rating 2 Star	5.9	7.5
Privacy Rating 4 Star	6.2	7.4*
Summary Factsheet	6.1	7.2**
Usage	5.7	7.4*
Costly Signal - Price	5.8	7.2**
Costly Signal - Fine	6.1	7.8
Info-label Combo - Below Average	5.9	7.5
Info-label Combo - Average	6.0	7.6
Info-label Combo - Above Average	6.0	7.4
Cool Down Period	6.6**	7.9

Statistically significant:

*** *at the 1% level* ** *at the 5% level* * *at the 10% level*

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

Willingness to share personal information (personalisation score)

Treatment vs. Control

TREATMENT	INDIA	KENYA
Control	6.7	8.0
Descriptive Norm - Simple	6.7	8.2
Descriptive Norm - Detailed	6.5	8.0
Descriptive Norm - Negative	6.4	8.2
Privacy Signal	6.7	8.3*
Anchoring	6.8	8.2
GC Blanket Consent	6.6	8.0
GC All Selected (Opt-out)	6.8	8.1
GC Essential Selected (Opt-in)	6.5	8.2

Statistically significant:

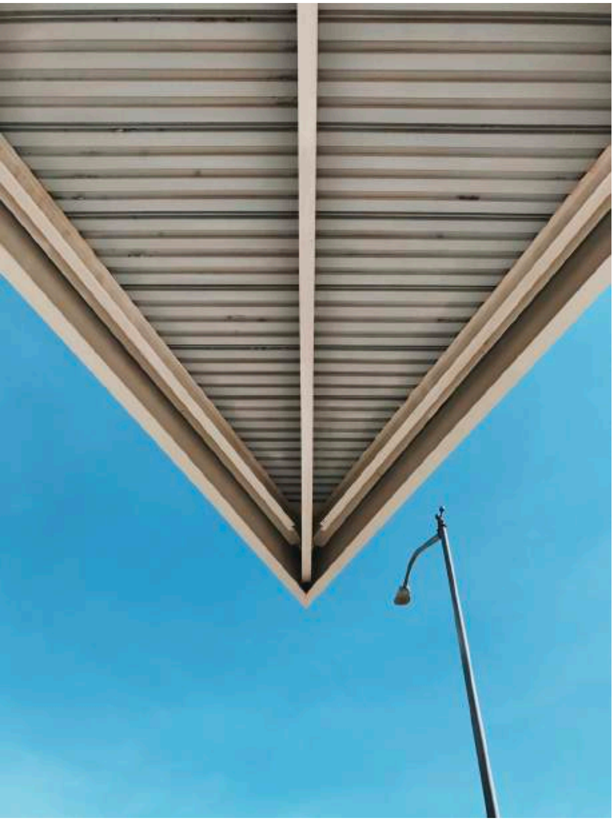
*** *at the 1% level* ** *at the 5% level* * *at the 10% level*

GC - Granular Consent

Statistical significance quantifies how confidently we can attribute results to our interventions rather than chance. The lower the significance level, the more confident we are of our results

CONTEXT IS KEY

Differences Between India and Kenya Results



1. Our control groups in India and Kenya were consistently different, reflecting that different socio-cultural factors in both countries influence how users approach privacy and data-sharing. Kenyans have a more vigilant approach to the privacy policy but also share more data, showing more trust in online data sharing as compared to Indians.

In the control group, Kenyan respondents report higher scores on all outcome variables than Indians i.e. Kenya respondents spend more time on the privacy policy, understand its terms better and share more sensitive and personal information.*

2. Treatment group respondents in Kenya shared personal information differently than respondents in India.

While Indians who were shown nudges such as star ratings, information labels, costly signals shared more personal information as compared to the control group (as expected), Kenyans who were shown these nudges shared less than the control group.

On the other hand, descriptive norm messages and granular consent nudges lead to higher personal information sharing by Kenyans compared to the control group, unlike Indians who ended up sharing lesser information, in most cases when shown the same nudges.

3. The impact of nudges on privacy behaviours is highly contextual - different nudges worked in India and Kenya

User data sharing behaviour was influenced by a range of nudges such as privacy signalling messages, usage case, the negative norm message and summary factsheet in Kenya. On the other hand, the cool down period nudge, which was our most deliberate or 'hard' nudge worked best in India.

** this is a directional finding not statistically significant*

NUDGING PRIVACY

Results and Implications | What worked

- The cool down period, which forced respondents to stay on the privacy policy for six minutes, and defaults, which created pre-decided sharing settings, are powerful tools to influence how much information consumers share. These “hard nudges” shape the environment in which users make sharing decisions.

  Implication: *Businesses and developers should focus on an integrated approach and redesigning the entire system within which data sharing decisions are made, rather than adding features or make small alterations to existing systems. This approach will be able to address several behavioural barriers at once and even have the potential to be personalised across different users. More specifically, defaults can be designed to keep the end user in mind. This will build trust between the customer and business, leading to better outcomes and more information sharing in the long-run.*

- What others do is very powerful. Both positive and negative ‘social norm’ messages had a significant impact on how much time people spent on the policy. It is human tendency to want to conform to behaviours exhibited by the larger community. When told majority of people spent more time on the policy or suffered because they did not, respondents were influenced to change their own behaviour.

  Implication: *Short messages or reminders which convey favourable behaviour of other users are useful tools to get individuals to do something. They are cost-effective and simple to implement. They can easily be added to existing service platforms and apps.*

Results and Implications | What worked

- Star ratings are an effective shortcut for consumers to understand how safe their data is with a platform or how much a service provider cares about protecting data. Our experiments have also shown us that higher star ratings can lead to more information sharing. This would be a great advantage for businesses to adopt as they will signal compliance to regulation and care for customer wellbeing.

  Implication: *While the exact format or features would have to be developed further, the rating holds an immense amount of potential. Consumers will be able to understand complex and abstract topics in a simple way, while businesses will have a standard to aspire to. The rating will have to be designed by regulators or a third-party to ensure that it is valid, trustworthy, and unbiased. Ratings will also have to be dynamic to account for growing size of the business, their changing revenue streams, and keeping them accountable over time, rather than just at a single point.*

Results and Implications | What might not work

- Many of the interventions that simplified information in the privacy policy [summary factsheet, granular consent] or disclosed consequences of poor privacy [costly signalling] were unsuccessful at making users read the policy in more detail, spend time on the policy, or alter their information sharing behaviour. While simplification is an important tool for behavioural scientists, it needs to be studied in greater detail in the field of data privacy. Based on these findings, we believe that data privacy is not solely an information gap but also a motivational challenge. People often do not want to take the initiative to know these things or spend more time deliberating their data sharing decisions.

  Implication: *Simplification needs to be accompanied by a harder nudge or change in the data sharing environment. For example, simplified versions of the privacy policy could be coupled with a cool-down or recommended default setting that holds the user's hand and leads them towards safer behaviours online.*

- Information about privacy is complex. Getting people to spend more time on the privacy policy [in case of social norm messages] did not lead to better understanding of its terms and conditions. Further, simplifying the policy [summary factsheet] did not lead to participants understanding policy terms better.

  Implication: *Reading a policy and understanding a policy are two different things. Businesses interested in building trust and remaining socially responsible will have to examine their customer profiles and think about the best way to make sure their customers are informed. This could take the form of videos or small audio clips for semi-literate populations or comic strips or simplified tools for semi-aware populations. The perfect solution will vary based on customer base and the business's intention. These ideas require further formative research and testing.*

Results and Implications | What requires further thought

Highlighting how data is used [usage case, blanket consent] or providing a summary of privacy policies [summary factsheet] make privacy terms salient. In Kenya, this led to users sharing less information, perhaps due to activating privacy concerns among participants. However, this does not mean that all similar nudges will lead to low data sharing. Showing how data is used is not guaranteed to lead to more or less data sharing.

Implication: *Usage cases tend to expose exactly how data is collected and shared, which gives customers a chance to understand what happens when they sign up to use an app. Adapting this solution will need to be thought about in more detail. Regulators might be the perfect stakeholder to get involved and mandate that how data is shared must be made clear in the consent form, preferably in a visual manner.*

RECOMMENDATIONS AND NEXT STEPS

Recommendations and Next Steps

Our experiments helped us learn a lot about users' privacy related behaviours. Here are our recommendations for what should come next, based on our deep analysis.

1

Further experimentation

Further development of nudges that have shown promise, like the star rating, to address weaknesses will help towards market readiness. There is a good scope to also combine treatments like the cool down period with a presentation nudge to seek better results.

2

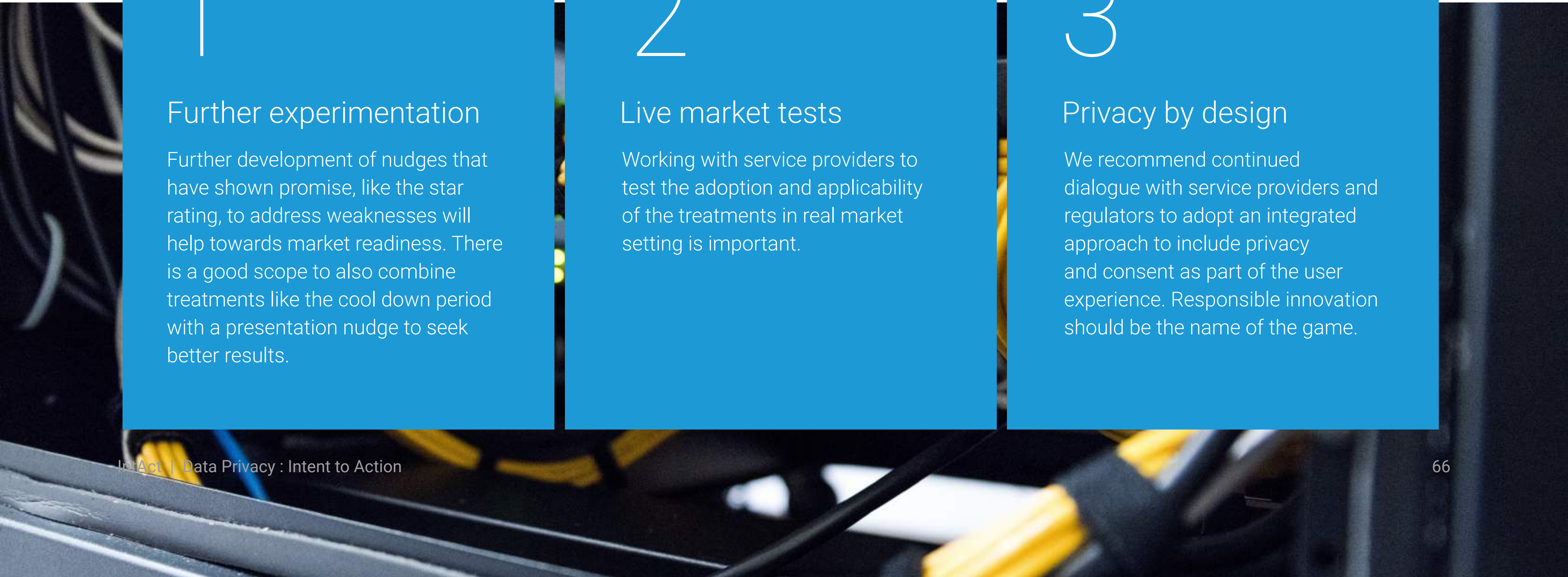
Live market tests

Working with service providers to test the adoption and applicability of the treatments in real market setting is important.

3

Privacy by design

We recommend continued dialogue with service providers and regulators to adopt an integrated approach to include privacy and consent as part of the user experience. Responsible innovation should be the name of the game.



CONCLUSION

Conclusion

Through our experiments, we learned that data privacy is a complicated concept for consumers to understand and make decisions about. They are often unaware or unmotivated to read detailed policies and spend time thinking about whether they should share information. At the same time, we found that hard nudges, such as the cool-down and defaults, can play a big role in shaping how consumers share data. We believe that consumers need to be assisted and taught about how to make better decision online. The responsibility cannot just fall on them. We recommend two methods of tackling this challenge: redesigning the choice environments in which consumers navigate data sharing online and involving regulators more.

Our evidence suggests that one strong solution could be developing a system of privacy ratings. These systems capture key information without excluding populations with low literacy or awareness levels. A system of standardized and dynamic ratings would not only ensure that users understand the privacy values of the apps or services they employ but also keep businesses accountable. We recommend that ratings be taken up by a credible independent agency or regulators with the goal of putting in place dynamic standards of privacy.

Our study also indicates that businesses could stand to gain from this. Introducing a cool down period or ratings seem to make users share more information - a win for both businesses and users. Beyond gaining the trust of the customers, businesses will also be able to use their privacy features to attract new users and gather more data consensually. As more people living in the global south move towards owning smartphones and tablets, user-centric businesses will lead the way in balancing user loyalty alongside their own priorities. In order to start designing for those advantages today, our next steps would be to run similar experiments on the cool-down, perhaps by combining it with other nudges. We would also recommend doing a live market test with privacy-conscious providers to see how consumers using an actual service respond to the concept of a cool down.

There is a long path ahead towards the perfect data privacy solutions, IntAct has set us on it by opening up avenues to imagine a future in which businesses and users can share the same priorities while achieving their respective goals. Our results have given us a glimpse into what that could look like. We are looking forward to applying these insights, designing and documenting privacy behaviours as well as working on our second round of interventions. We hope our work will one day become part of a larger body of privacy research that makes the world a better and safer place for all.

RESEARCH BY

Busara

The Busara Center for Behavioural Economics is a research and consulting firm that applies and advances Behavioural science to address the most challenging development problems in India and across Africa. Busara works with academics, policymakers, and organizations to evaluate and implement Behavioural and social interventions. Busara has consistently improved its partners' products, programs and had policy impact across a number of sectors, including financial inclusion, health, agriculture, and governance.

www.busaracenter.org

Centre for Social and Behaviour Change

Centre for Social and Behaviour Change (CSBC) at Ashoka University is set up by a grant from the Bill and Melinda Gates Foundation (BMGF). The vision of the Centre is to establish an institution in India that is globally reputed for thought leadership and excellence in impactful behaviour change interventions for poor and marginalized populations. CSBC works in the areas of nutrition, sanitation, maternal health, family planning, financial inclusion and data privacy through a mix of behavioural change programmes, capacity building and foundational research. They have set up the Behavioural Insights Unit for the Government of India at the NITI Aayog in partnership with BMGF to improve development indicators on the ground using behavioural insights.

www.csbc.org.in

SUPPORTED BY

OMIDYAR NETWORK

Established by philanthropists Pam and Pierre Omidyar, Omidyar Network is a social change venture that has committed more than $1 billion to innovative for-profit companies and nonprofit organizations since 2004. Omidyar Network works to reimagine critical systems and the ideas that govern them, and to build more inclusive and equitable societies in which individuals have the social, economic, and democratic power to thrive.

www.omidyar.com

OMIDYAR NETWORK INDIA

Omidyar Network India invests in bold entrepreneurs who help create a meaningful life for every Indian, especially the hundreds of millions of Indians in low-income and lower-middle-income populations, ranging from the poorest among us to the existing middle class. To drive empowerment and social impact at scale, Omidyar Network India works with entrepreneurs in the private, nonprofit and public sectors, who are tackling India's hardest and most chronic problems. This is in addition to, making equity investments in early stage enterprises and providing grants to nonprofits in the areas of Digital Identity, Education, Emerging Tech, Financial Inclusion, Governance & Citizen Engagement, and Property Rights. Omidyar Network India is part of The Omidyar Group, a diverse collection of companies, organizations and initiatives, supported by philanthropists Pam and Pierre Omidyar, founder of eBay.

www.omidyarnetwork.in

www.intactprivacy.com | Twitter: @IntAct_Privacy

IntAct
Data Privacy : Intent to Action