callsign®

GET ON

INTELLIGENCE BEYOND RECOGNITION

Use Case

What is Invasion of Privacy?

An invasion of privacy occurs when there is an intrusion upon a person's reasonable expectation to be left alone.

What Is Choice, Consent and Control?

Choice – is the ability for a user to select identification and authentication methods, considering that they have the technology, location and preference to use each method.

Consent – is the recording of the user's selection of the preferred authentication methods

Control – is the ability of the user to determine under what circumstances an identification or authentication method can be deployed; and their ability to change these methods, easily and quickly.

What is Personally Identifiable Information (PII)

PII is any data that can be used to identify, contact or locate a specific individual. It is also be known as Sensitive Personal Information (SPI).

Turning Users into Security Advocates with Choice, Consent and Control

As security professionals we know that binary authentication just doesn't work. Whether it is a username and password combination, or a biometric that can be replicated - or hacked and replaced. We also know that some users are deeply suspicious of certain authentication factors that can be seen as invasive. The Callsign 2018 Annual User Identity Preference Survey showed that passwords were still the number one choice of users surveyed, no matter what their demographic. The fact is that users see security, and the surrounding regulations as someone else's problem - their banks', their employers', the companies they buy from.

What users do care about is their privacy. In every news feed there are stories raging against invasion of privacy instances. Be it a company in Illinois, being sued by an employee for breaking the state's biometric information privacy act, border guards in Canada being able to demand passwords to check entrants' laptops, or police in London for their use of facial recognition. So how can security professionals balance user privacy and security?

Let's add another layer to this balance, the frictional layer. Users want to be secure, to manage their privacy, and also for the security to be as invisible as possible, without compromise.

Regulations increasingly stipulate that users must **Consent** to their information being used, and that they have ability to **Control** that use. Only having options of consent and the ability to control the consent (i.e. the right to be forgotten) present security challenges, and so concepts such as legitimate need are applied, to override preferences. The answer to balancing, security, privacy and friction comes in the level of involvement you allow users to have.

This is where the 3rd element plays such an important part. **Choice**, and the ability to control the choices we make as users. By offering users the ability to choose their method of authentication, and which pieces of personally identifiable information PII is used, e.g. email address, or date of birth; it is possible for users to choose the level of friction they are willing to go through in the authentication journey. Choice is also important as not all users have access to a smart phone, or have access to a computer in their home.

With this comes a need to educate users on what the choices mean, how some methods of authentication, like behavioural, are harder to replicate than others. How some actions they perform, and when and where, may indicate the need for increased authentication, but equally, how some actions can be accomplished friction-free. This is where security professionals on customer and vendor sides need to work together.

> At the heart of these challenges is the need to prove someone is who they say they are, where they say they are, doing what they say they are doing. Checked and verified to keep them safe, or held to account.

Is your organization facing an Identity Paradox?

Until now organisations believed it was impossible to satisfy the conflicting needs of security, accountability and privacy.

Regulators

Regulators are enforcing compliance with regulations like GDPR and PSD2.

Organizations

Organisations need to keep identity data safe and be accountable for doing so.

Users

Users want increasingly seamless, friction-free authentication journeys.

Giving Users Choice, Control And Consent with Callsign

Callsign's platform combines our intelligence, decisioning, authentication and verification modules which deliver:

Personalized User Authentication Journeys

Using interactions that suit the demographic and user preferences.

Security

Callsign can confirm that the user really is who they say they are, with no false positives.

Control

With an irreputable audit log of user consent, choice and control, and management of data collected.

Real-time Identification

Correlating the location, devices and behavior of applicants.

Dynamic Authentication

By defining a specific authentication journey depending on user, activity or context.

Anonymised Data

Callsign can verify the user, without knowing them.

Callsign changes the rules of identity. By using all of the thousands of data points available, such as typing or swiping techniques, location, online habits, face recognition, devices, and yes, even passwords, we can determine someone is who they say they are. We even know the Monday person can behave differently from the Friday person.

Most of these data points are friction-free for the user, and so we use these to determine that someone's behaviour is within their normal pattern. Where there is a veering from the norm, we then intelligently introduce further tests, avoiding a rules-based approach that can be replicated by the bad guys. We have the lowest false positive rates in the industry, and zero breaches thanks to our inbuilt trust engine. As a result, users can get on with their digital lives whilst businesses improve customer engagement, increase productivity and reduce the risk of fraud.