



# DATA SIGNALS

## BLOCKCHAIN BASED DATA ACCESS CONTROL

GARY MAWDSLEY CEO  
DMITRY TISHKOVSKY CTO

Personal data is being weaponised, the ultimate consequence of which is surveillance of the individual.

Data privacy remains a huge problem, and up until now the data subject (the owner of the data) has never been in control. The capture, storage and processing of an individual's data is currently in the hands of corporations. Brilliantly drafted legislation such as the GDPR focuses on providing the individual with rights, ensuring institutions work to a standard code of practice with very specific reference to the privacy of the individual.

Data Signals have created two products that together address key issues of data privacy: pseudonymisation and frading (BluMamba), and differential privacy (PinkScorpion), thereby placing data access control into the hands of the individual. BluMamba and PinkScorpion are not restricted to personal data and have great resonance with the goals of the many territorial privacy laws. The techniques embodied can be applied to numeric, character and binary data including audio and video.

PinkScorpion controls access to an individual's data using an electronic contract stored and executed on the Blockchain. The Blockchain is a

processing and storage mechanism that is not under the control of single commercial or governmental organisations. Instead it works using an independent set of controllers all competing for a reward achieved by storing information in to a chain of blocks. Due to the difficulty (compute cost) in maintaining the chain of blocks it is extremely difficult (if not impossible) to alter the historical records in the chain retrospectively, i.e. history cannot be re-written. The chain forms the definitive record of events. PinkScorpion uses this to record the dates, times, and organisations making access to an individual's data.

PinkScorpion uses the electronic contract you agreed with the service providing organisation (e.g. your bank) to ensure only the attributes required by an agreed service are released using a timelock from their storage silos for inclusion in processing. At any point the individual can terminate the contract resulting in the disconnection of the data from the service providers processing engine.

PinkScorpion audits [to the Blockchain] every access request made of data, allowing the data subject to see when and whom accessed their data, and under which contract. Any funny business shows up immediately. Access logs are obfuscated and encrypted on the blockchain.