The Identity Salon™

Identity Salon October 2024

Recap and Insights

Executive Summary

The inaugural Identity Salon™ brought together a mix of identity and security professionals and policymakers under the Chatham House Rule for an open, honest conversation about the big issues shaping digital identity today and ways to address those issues with the right stakeholders over the coming years. Held alongside the Authenticate Conference, this half-day summit invited participants to tackle challenges ranging from managing digital estates after death to the evolving role of AI in fraud detection and identity management.

Discussions highlighted several key themes. There was a lively debate on where identity should sit within organizations as the lines between security and operations continue to blur. Participants also explored the role of AI in identity and access management (IAM), recognizing its power to detect threats while pointing out the need for skilled humans to interpret and act on AI-driven insights. The event helped emphasize the importance of IAM's role across different functions, raising important questions about how organizations should structure these teams and the cultural shifts needed to break down silos.

This report captures the insights and ideas shared at The Identity Salon, offering recommendations for industry and academic collaborations that could drive progress in these complex areas. It sets the stage for future salons, aiming to turn this gathering into a key space for addressing the big, long-term questions in digital identity.

The organizers would like in particular to thank SGNL, AKA Identity, Beyond Identity, and Natoma for their generosity as signature sponsors; and to recognize the FIDO Alliance for their unwavering support.

The ultimate goal is to have tools that allow enough granular control, letting someone say what they want to have saved, who they want to have access to, and what should be deleted. There won't be a set of prescribed rules that works for everyone, so we need tools that will allow choice and flexibility.

The DADE Community Group

The OpenID Foundation has a new group focused on this area: the Death and the Digital Estate (DADE) Community Group. It has brought together a variety of resources from people and organizations that have started to discuss some aspects of this problem. It is organized based on the following principles, one of which the group suggested be revised:

- Respect for different perspectives
- Empowerment through consent
  - The group suggested changing "consent" to "choice," as the word "consent" has been overloaded over the last few years. "Choice" implies a much more active decision.
- Interoperability and Accessibility
  - Whatever we come out with, we need to promote interop between platforms to facilitate seamless data management across systems. We need common ways to talk about these things and organize around the patterns.

Further Questions

This is an emerging area, which means many open questions are ripe for discussion.

- What happens to people who have been identified as deceased and who are in fact alive?

- If the digital data overlaps a physical device (e.g., a smart thermostat), what does the transference of that device (and its data) look like? Is the death of an asset the same as the transference of an asset? Could you use the same mechanisms in either case?
- What about the 'death' of non-person and machine entities (e.g., decommissioning a physical machine like a car)?
    - To be clear, when an autonomous vehicle is no longer on the road matters. If someone claims it was in an accident, the authorities need to know it wasn't on the road. In the case of something like a drilling rig, it won't have the same registration that a car would, but—for cybersecurity and for compliance reasons—authorities still need to know if it's no longer a valid asset.

Understanding and handling death and the digital estate is a problem for identity; it is not, however, an identity management problem per se. It won't be solved solely by identity management, but whatever our industry does in this space will impact digital identity overall.

Supplemental Research and Industry Perspectives

This topic is not new, but it is gaining urgency. Reviewing research literature sees content going back over a decade as people started to consider what to do with their digital estate. In John Conner's paper, "Digital life after death: The issue of planning for a person's digital assets after death," published in 2010, he focused on email, social media, and blogs. His recommendations focus more on pre-planning and individual agency, including leaving access information and instructions, setting up a trust, and providing some information about digital assets in a will. There was no thought to a more global, legally supported pattern.

Thinking continued to evolve, however, particularly in the U.K. Heather Conway and Sheena Grattan wrote a paper, published in 2017, called "The 'New' New Property: Dealing with Digital Assets on Death." This paper focuses on defining the concept of "digital asset" and then dives into the challenges posed in managing them from an estate planning perspective. The U.K. has notably complicated succession laws that span use cases from centuries ago to today. Interestingly enough, however, the authors point to the United States' Uniform Fiduciary Access to Digital Assets Act (now the Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA)) as a model to follow.

[1] Connor, John, Digital Life after Death: The Issue of Planning for a Person's Digital Assets after Death (December 1, 2010). Texas Tech Law School Research Paper No. 2011-02, Available at SSRN: https://ssrn.com/abstract=1811044 or http://dx.doi.org/10.2139/ssrn.1811044

[2] Conway, Heather and Grattan, Sheena, 'The 'New' New Property: Dealing with Digital Assets on Death' (2017). Conway (with Sheena Grattan, BL), "The 'New' New Property: Dealing with Digital Assets on Death" in Conway and Hickey (eds), Modern Studies in Property Law, Volume 9 (Hart Publishing, July, 2017) pp 99-115 , Queen's University Belfast Law Research Paper No. 2021-126, Available at SSRN: https://ssrn.com/abstract=3289171

"The Revised Uniform Fiduciary Access to Digital Assets Act (RUFADAA) governs access to a person's online accounts when the account owner dies or loses the ability to manage the account. A fiduciary is a person appointed to manage the property of another person, subject to strict duties to act in the other person's best interest. Common types of fiduciaries include executors of a decedent's estate, trustees, conservators, and agents under a power of attorney. This act extends the traditional power of a fiduciary to manage tangible property to include management of digital assets. The act allows fiduciaries to manage digital property like computer files, web domains, and virtual currency, but restricts a fiduciary's access to electronic communications such as email, text messages, and social media accounts unless the original user consented to fiduciary access in a will, trust, power of attorney, or other record."

The Uniform Law Commission

This only applies to U.S. states; the RUFADAA is not something that has been adopted more broadly. It is also worth noting that it does not cover all the digital assets the participants of The Identity Salon identified during our discussion. It is, however, an interesting place to start considering a more standardized regulatory approach.

Moving to another part of the world, Prashant Mali and Aswathy Prakash G., wrote "Death in the era of perpetual digital afterlife: digital assets, posthumous legacy, ownership and its legal implications," published in 2019 through the National Law School Journal (NLSJ) at the National Law School of India University. These authors, as with many others, focus on defining what constitutes digital assets and expands that definition quite a bit.

- **Personal Digital Assets:** emails, documents, photos, videos, contacts, loyalty reward points
- **Financial Digital Assets:** online banking data, associated usernames and passwords, records of online financial transactions, investments, virtual properties, goods of value traded in online gaming platforms, e-wallets payments given for online gambling, digital, virtual and crypto currencies like Bitcoin, Ether (ETH).
- **Professional Digital Assets:** domain names, official email accounts, social media handles, blog and web content, visual content and other content management system (CMS) used, customer database of online businesses, auction sites, etc.
- **Technical Digital Assets:** passwords for various digital services, computer networks, device backup logs: both local and cloud based, web hosting services, software projects: both enterprise and individual, etc.

It goes another step, however, and considers issues of identity theft and copyright violations of deceased user's accounts. The non-closure of accounts leads to the possibility of account takeover in a way that leaves no one (except the attacker) the wiser. Laws may protect legal heirs from liability, but the considerations go beyond liability; emotional and mental well-being are also an issue. This is definitely a paper to review if you are further interested in the topic.

There is quite a bit more written by scholars and researchers, but what laws and regulations exist continue to build off of the precedent of physical assets and succession laws. Unfortunately, what works for physical assets does not always work for digital ones, leaving some significant gaps both in the laws and in the technology needed to support those laws.

[3] Mali, Dr Prashant and G, Aswathy Prakash (2019) "Death in the Era of Perpetual Digital Afterlife: Digital Assets, Posthumous Legacy, Ownership and its Legal Implications," National Law School Journal: Vol. 15: Iss. 1, Article 8. Available at: https://repository.nls.ac.in/nlsj/vol15/iss1/8

About The Identity Salon

The Identity Salon™ provides a unique, exclusive environment where seasoned digital identity architects, technical standards experts, and researchers can engage in meaningful, protected conversations. Limited in size to foster genuine connections, this gathering allows experienced professionals to dive into complex, long-term challenges with peers who understand the depth and breadth of identity's impact.

We host the Identity Salon under the Chatham House Rule, facilitating candid dialogue that often isn't possible in larger, more public settings. Participants have the rare opportunity to explore the '5-year problems' in identity, share leading practices, and discuss emerging approaches with like-minded experts. Our aim is to bridge the gap between academic and industry research and real-world practice, connecting public and private sectors to advance knowledge and drive practical solutions.

Why do we do this? As identity becomes mainstream, industry events are increasingly geared toward newer practitioners, leaving few spaces for seasoned professionals to collaborate on advanced issues. The Identity Salon fills that gap. After each event, we publish post-event reports that summarize discussions and insights, ensuring our conversations have a lasting impact on the field.

The Identity Salon is conceived and curated by:

Heather Flanagan, Principal at Spherical Cow Consulting, who comes from a position that the Internet is led by people, powered by words, and inspired by technology. She has been involved in leadership roles with some of the most technical, volunteer-driven organizations on the Internet, including IDPro as Executive Director and Principal Editor; the OpenID Foundation as Lead Editor; the IETF, IAB, and the IRTF as RFC Series Editor; ICANN as Technical Writer; and REFEDS as Coordinator, just to name a few.

Ian Glazer, the founder and president of Weave Identity – an advisory services firm. Prior to founding Weave, Ian was the Senior Vice President for Identity Product Management at Salesforce. His responsibilities include leading the product management team, product strategy and identity standards work. Earlier in his career, Ian was a research vice president and agenda manager on the Identity and Privacy Strategies team at Gartner, where he oversaw the entire team's research. He is a Board Emeritus and the co-founder of IDPro, and works to deliver more services and value to the IDPro membership, raise funds for the organization, and help identity management professionals learn from one another. Ian is also a Board of Directors member and cofounder of the Digital Identity Advancement Foundation, focusing on removing financial barriers to participation in the digital identity industry. During his career in the identity

industry, he has co-authored a patent on federated user provisioning, co-authored and contributed to user provisioning specifications, is a noted blogger, speaker, and photographer of his socks.

Andrew Hindle, an independent consultant focusing on digital identity, cyber security, privacy, and corporate governance, through Hindle Consulting Limited. Andrew is the Identiverse Conference Chair, and serves as a member of the board at Curity and at Kantara. He has over 25 years' experience in the software industry in a range of technical sales, pre-sales, product marketing, business development and corporate governance roles. He maintains CIPP/E, CIPM and CIPT privacy certifications with the IAPP; a CIDPRO certification from IDPro; and holds a BA in Oriental Studies (Japanese) from Oxford University and an advanced professional diploma in corporate governance. Outside of the world of identity, Andrew is Chair of Trustees for his local scouting group, rides regularly with a local road cycling group, and plays keyboard, guitar and bassoon (not at the same time) with more enthusiasm than skill, and for an audience of one. Andrew is based in the UK.

Thanks to our 2024 Supporters!

Awesome

sgnl

Fabulous

BEYOND IDENTITY

aka identity

natoma

Splendid

Hindle Consulting

Spherical Cow Consulting

Weave Identity