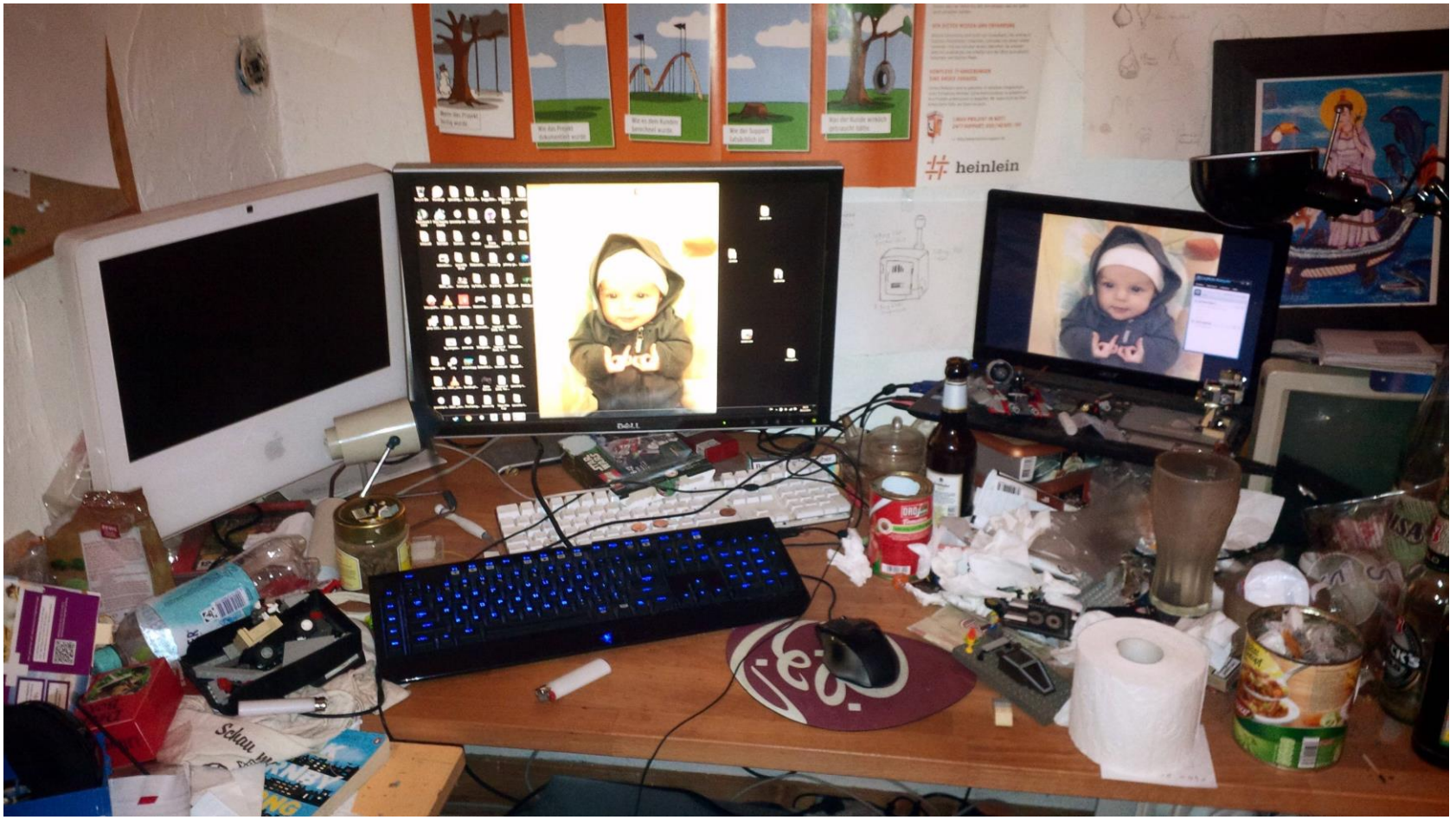
RESO Fall Conference

Data Distribution Best Practices

Amy Gorce & Kevin Greene

Bad Set-ups

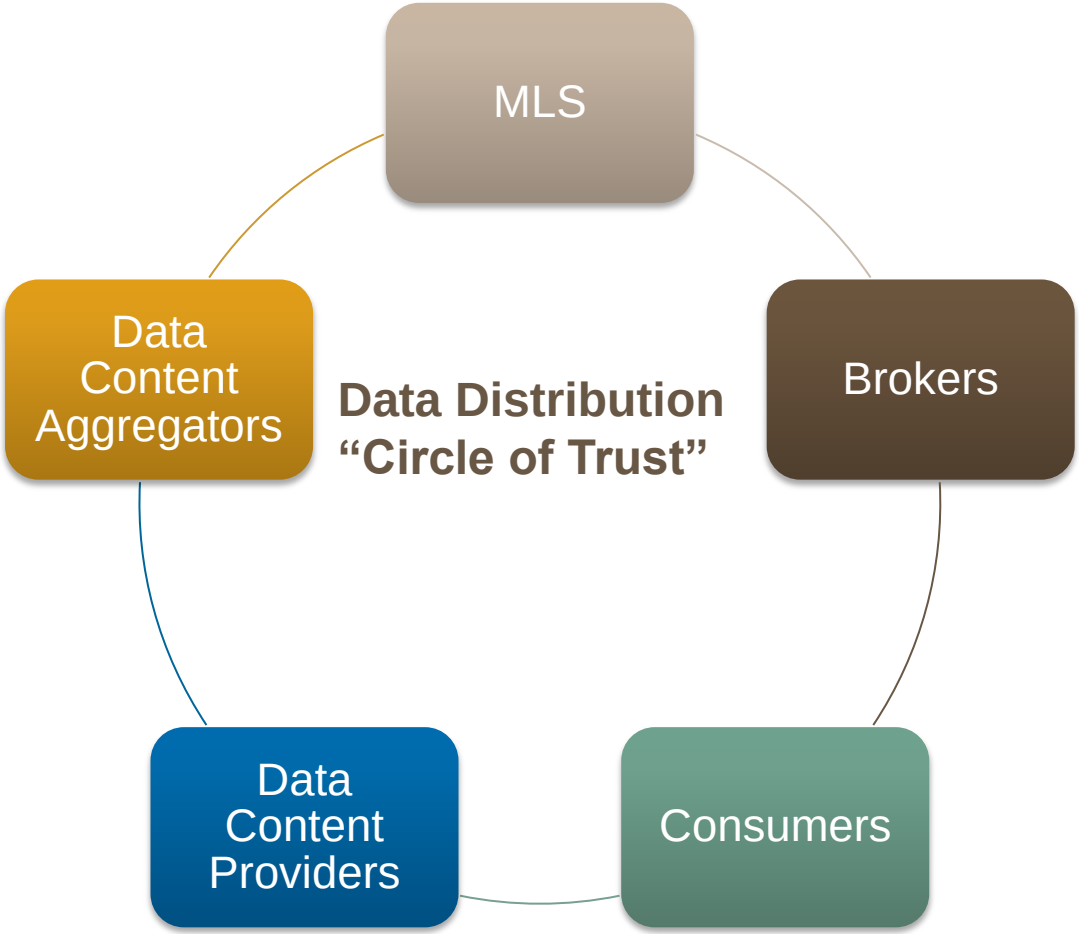


Best Practices in Data Distribution

- Why are best practices needed?
- What can my MLS do to get started?

RESO Standards	Solid Legal Foundation	Resource: RETS R&D Workgroup	Resource: CMLS Best Practices
Best Practices Setup	Best Practices Compliance	Best Practices RETS Creds	Best Practices Enforcement

Let’s start with what the challenges are today



Why standards are critical for data distribution

- Removes friction with brokers and technology partners
- Enables rapid innovation
- Reduces support and compliance efforts
- Improved security

RESO R&D Workgroup 2017 – Best Practices

- Review and update data access rules and restrictions as needed to accommodate (real time) API access
- Request/require data consumers change their access passwords/passphrases biannually.
- Require data consumers secure all credentials and data stored.
- Provide URI (CDN) based media and request/require data consumers use the URI in real-time

Council of MLS Best Practices - Data Licensing

- Scope of and access to the licensed data.
- Use of the licensed data.
- Protection of the licensed data.
- Intellectual property rights and ownership rights.
- Fees.
- Compliance.
- Confidential information.
- Warranties and representations.
- Indemnification and limitation of liability.
- Term and termination.
- Audit rights.

CMLS
Council of Multiple Listing Services

Council of MLS Best Practices - Security

- Compliance with security standards (e.g. different levels of the OWASP Application Software Verification Standard)
- Operating system, cloud, web server, and database hardening standards and best practices
- Patching and upgrade practices
- Anti-scraping (per OWASP best practices)
- Software features based on security requirements (e.g. export limits, data retention, encryption)
- Credential security
- Transport encryption
- Firewalling and secure protocol use
- Secure storage and disposal

CMLS
Council of Multiple Listing Services

Council of MLS Best Practices – Compliance & Enforcement

- Content retention –, storage of images vs. use of an image content delivery network controlled by the data provider; length of retention in production environments and backups past that needed for allowed uses.

- Compliance reviews – initial and ongoing, cure period for issues, compliance costs and fines.

- Notification of significant change to usage (e.g. website or app major release; new features using licensed content).

CMLS
Council of Multiple Listing Services

Best Practices - Setup

- Each data consumer is tied to an agreement.
- Agreements are also tied to the data provider itself (for a site license) or individual subscriber.
- Management of license agreements includes all of the details necessary for easy compliance reviews
- Data feeds follow the principle of “least privilege” where data consumers receive only the content they need
- Re-signing new versions or addendums is easy and compliance with this requirement is easy to monitor.
- Payment of fees is secure (PCI DSS compliant) and easy to monitor.

Best Practices – Compliance Monitoring

- Establish a process for determining when data consumers undergo compliance review, in addition to when there is a complaint.
- Compliance monitoring policy should address pre and post implementation reviews as well as periodic reviews.
- Establishing consistent review procedures and scope that matches the auditable criteria laid out in data license agreements and data usage rules.
- Ideally compliance tools are built in or integrated with data distribution platform.

RETS Credential Usage Policies

- Pros and cons to allowing re-use but generally best to tie credentials to a license and a feed.
- Auditing and enforcement mitigate arguments for issuing individual RETS creds per member vs. per data consumer.
- Watermarking and data seeding add some value but don’t “solve” the whole problem.

Best Practices RETS Credential Security

- Review excessive use of RETS credentials.
- Lockdown access to IP or IP range.
- Evaluating RETS client “fingerprint” is as expected.
- Credential change management.
- Carefully track use of API keys to mitigate key faking or interception.
- TLS implementation best practices.

Best Practices RETS Credential Security

- Protect against attack on Oauth tokens and shared-secrets by using long and random values
- Attack lockouts for accounts, including notification.
- Monitor for credential stuffing (especially use of non-unique credentials).
- Instrumentation to handle attack detection and automated response (which may include Oauth key revocation and other methods).
- Testing and evolution of security tools and requirements

Best Practices in Enforcement

- Penalties should “fit the crime”.
- Consistent application of penalties is critical.
- Mitigate enforcement through education and clear documentation.
- Documentation of enforcement steps taken to preserve “history”.
- When assessing penalties to members, be aware of MLS Policy guidelines
- Responsibility if it is discovered that the content consumer has experienced a breach.

Sweet Set-ups