Анализ · 16 мая 2026 г.

← Предыдущий·Следующий →

Шифрование не означает конфиденциальность: что метаданные говорят о вас

Зашифрованное содержимое и видимые метаданные — это две разные вещи. Когда сервис говорит о «сквозном шифровании», он рассказывает только половину истории.

Замок, который не защищает все

Большая часть современных мессенджеров рекламирует сквозное шифрование. И это правда: содержимое сообщений передается зашифрованным, так что никто в пути — даже поставщик услуг — не может прочитать текст во время передачи. До этого момента утверждение является точным.

Проблема в том, что содержимое — это только часть истории. Даже если никто не может прочитать то, что вы говорите, сервис знает другие вещи с очень высокой точностью: с кем вы разговариваете, в какое время, как часто, из какого примерно местоположения, на каком устройстве, сколько сообщений вы отправляете и сколько получаете, сколько файлов вы передаете. Все это называется метаданными (metadata). И метаданные во многих случаях говорят почти столько же, сколько само сообщение.

Что раскрывают метаданные

Не нужно читать сообщение, чтобы знать многие вещи. Если человек звонит или пишет онкологу каждое вторничное утро в девять часов в течение шести месяцев, не обязательно слышать разговор, чтобы догадаться, что происходит. Если два человека обмениваются сотней сообщений в день и вдруг прекращают это делать, не нужно читать ни одного, чтобы понять, что произошло. Если налоговый консультант получает двадцать сообщений подряд от одного и того же клиента в ночь перед квартальным закрытием, шаблон говорит сам за себя.

Метаданные раскрывают поведенческие модели: кто с кем в отношениях, какие графики у каждого человека, когда они бодрствуют, когда спят, когда путешествуют, какие клиенты наиболее активны, какие профессиональные отношения наиболее интенсивны. Сервер, собирающий метаданные, может построить детальный профиль личной и профессиональной жизни любого пользователя, никогда не прочитав ни одного слова из того, что он пишет.

Есть исторический пример, который иллюстрирует это жестко. Бывший директор NSA Майкл Хайден сформулировал это прямо в 2014 году: *«We kill people based on metadata»*. Заявление касалось военных операций США против целей, идентифицированных исключительно на основе их моделей коммуникации. Ни одного прочитанного сообщения. Только граф контактов и графики.

То, что сервис собирает метаданные, не обязательно означает, что он будет использовать их против своих пользователей. Это означает, что он имеет такую возможность, и что третья сторона с доступом к этим данным — по решению суда, из-за нарушения безопасности или через продажу третьим лицам, если условия предоставления услуг это позволяют — также имеет ее.

Доступ к адресной книге

Еще один вектор, который проходит почти незамеченным: список контактов. Большая часть мессенджеров просит доступ к адресной книге телефона при регистрации. Они загружают все номера на свой сервер, чтобы показать, кто еще пользуется сервисом. С этого момента у компании есть полная карта отношений пользователя, даже если он никогда никому не написал ни одного сообщения.

Для профессионала, на которого распространяется профессиональная тайна — адвоката, врача, психолога, консультанта — эта адресная книга содержит клиентов. Если адресная книга была загружена на сервер третьей стороны, имена клиентов находятся в инфраструктуре, юрисдикцию и политику которой профессионал не контролирует. Профессиональная тайна не нарушается в тот день, когда кто-то сливает разговор: она была нарушена гораздо раньше, в момент согласия на загрузку.

Разница между шифрованием и несбором

Шифровать — значит защищать содержимое. Быть частным — значит не собирать то, что не нужно. Это разные вещи, и разница является операционно решающей. Сервис может идеально шифровать все сообщения и одновременно знать почти все о своих пользователях через метаданные. Оба варианта вполне совместимы. На самом деле это доминирующая бизнес-модель в секторе.

Правильный вопрос для оценки истинной конфиденциальности сервиса — не *«шифрует ли он содержимое?»*. На этот вопрос ответ известен уже много лет. Правильный вопрос такой: *«какие метаданные он генерирует и где они хранятся?»*. И, прежде всего: *«какие метаданные ему не нужно генерировать?»*.

Архитектура, которая минимизирует метаданные по дизайну (privacy by design) — не по обещанию, не по внутренней политике — является структурно более частной, чем архитектура, которая их собирает и шифрует. Потому что данные, которых не существует, не могут быть слиты, проданы, переданы по решению суда или потеряны при взломе.

Для профессионального читателя

Если ваша профессиональная деятельность связана с тайной, конфиденциальностью или просто уважением к информации третьих лиц, стоит задать вопросы в таком порядке:

1. Шифрует ли приложение, которое я использую для общения, содержимое? (Вероятно, да.)
2. Шифрует ли оно метаданные? (Вероятно, нет.)
3. Генерирует ли оно метаданные, которые ему *не нужны* для работы? (Почти наверняка, да.)
4. Где хранятся эти метаданные и под какой юрисдикцией? (Вероятно, за пределами Европейской экономической зоны.)
5. Знает ли мой клиент или пациент, что его данные там?

Последний вопрос — неудобный. Потому что честный ответ в большинстве случаев: нет.

Эта статья является первой в серии о реальной работе профессиональных инструментов коммуникации. Следующие выпуски будут посвящены соблюдению GDPR в мессенджерах и концепции профессиональной тайны в цифровую эпоху.

Источники и дополнительная литература

- Хайден, М. — Заявление в Университете Джонса Хопкинса, 2014 г. («We kill people based on metadata»). Доступны публичные стенограммы.
- GDPR (Регламент ЕС 2016/679), ст. 4 и 5 — определение персональных данных и принципы обработки (метаданные являются персональными данными).
- Европейский инспектор по защите данных и EDPB — заключения по обработке данных трафика и метаданных в электронных коммуникациях (директива ePrivacy).

← ПредыдущийКраткая история сургучной печатиСледующий →Профессиональная тайна в цифровую эпоху

Недавние материалы

- CUADERNOS_LIST_PREGUNTAS_TITLE
- CUADERNOS_LIST_SELFHOST_TITLE
- CUADERNOS_LIST_IDENTIDAD_TITLE

Возьмите эту статью с собой туда, где она вам понадобится.

↓ Markdown ↓ Простой текст ↓ PDF

Файл будет загружен на ваше устройство. Оттуда вы можете сохранить его, импортировать в Solo2 или поделиться им где угодно. Cuadernos не решает место назначения за вас.

Сургучная печать · SHA-256 a58c733125e492afece7f46d33da87d891a5a8889980f84a74a62aa1df84cc35

Cuadernos Lacre · Издание Menzuri Gestión S.L. ·
текст R.Eugenio · под редакцией команды Solo2.