Privacy – it's all about balance

Strategies for an Evolving World
2008 NSS Conference
St. John's, Newfoundland and Labrador
3 June 2008

Suzanne Morin
Bell Canada

A practical approach to balancing privacy

1. **PIPEDA**
   - Standard gone law
2. **Perspectives on outsourcing**
   - Four key steps
3. **Building privacy into technology**
   - Case study: Voice Identification Service (VIS)

1. PIPEDA – Standard gone law

- **CSA Privacy Standard (NSC)**
  - Essentially management system type standard
  - All about supporting business practices
    - Fair information practices tailored to business
    - Flexibility needed as one size does not fit all
  - Difficult to conduct a “privacy audit” per se
    - Every privacy obligation tied to a business/commercial practice
    - Focus on specific areas: e.g. contractual safeguards when outsourcing to 3rd parties

No more “privacy” standards

- **Other standards should respect principles of privacy standard**
- **Focus on tangible areas**
  - E.g security/encryption – so when used, aids with privacy compliance, but not compliance in and of itself
- **Technical standards seen as the “tools” to implement principles in privacy standard**
  - avoids costly retrofitting of products and services
- **Privacy standard can assist in bridging the gap between those countries with legislation and those without**

2. Perspectives on Outsourcing

- PIPEDA does not prevent companies from outsourcing to Cdn, US or foreign service providers or parents
  - but does require companies to be transparent and they must protect this information to the extent possible by contractual and other means

- Consider a business function as a candidate for outsourcing ONLY if the benefits of outsourcing the business function outweigh the associated risks

Four Keys to Outsourcing

i. Verify

ii. Minimize

iii. Anonymize

iv. Notify

i. Verify

- Do your due diligence
  - Investigate service provider (e.g. privacy policy, trains employees, ability to provide comparable level of protection)
    - very relationship between employer/employees important
    - visit sites and conduct on site due diligence to satisfy self proper restrictions are in place
    - review all of suppliers processes and procedures and prepare deficiency list in the event deficiencies are discovered and require supplier to rectify before launching services
  - Pay particular attention to legal requirements of jurisdiction, as well as social, economic and political conditions that may impact service provider's ability to provide service/s
    - Geopolitical risk: high, medium or low risk
    - What are privacy laws in foreign jurisdiction?
- Assess overall level of risk associated with various services being outsourced across the Company

ii. Minimize

- Minimize disclosure and storage to U.S./foreign vendors of only that customer information absolutely necessary to carry out, on your behalf, function with which they have been tasked
  - fundamental best practice in privacy circles
  - something we've been doing (or should have been doing) for years
- convenience is NOT good enough
  - E.g. walk through each and every data field to determine if necessary
- if access to database is necessary, consider limiting access on a query basis rather than full access to entire database, or limiting access to read only with no ability to make changes
- consider storing data on a separate server in Canada and granting vendor access to database from abroad – this way allows you to shut down access from abroad if necessary
- Give parameters, but ultimately a business decision
- Depends on "materiality"

iii. Anonymize

- Wherever possible, anonymize customer information sent to U.S./foreign vendors
- Use separate unique identifiers that only mean something to you
- Take pains not to provide US/foreign vendor with information that would allow them to identify individual subscribers
  - e.g., while vendor may have log information, may not have full profile information to match with a named individual, tied to a phone number and address
  - makes it impossible for U.S./foreign authorities to identify individual customers, without the aid of Canadian law enforcement/courts through the Mutual Legal Assistance Treaty, etc.

iv. Notify

- Notice to customers that when they use the service in question, data may be stored in the U.S/other jurisdiction (see next slide for sample language).
  - Customers typically cannot withdraw their consent from such clauses
  - Query whether such high level notices provide any value to customers given extent of outsourcing
  - still goes to transparency – now a best practice under PIPEDA
- May be useful to include similar language in user agreements for particular services where there is some additional sensitivity to the data being provided cross-border
  - e.g. location-based services.
- Similar notice for employees so that they at least know about the possibility
  - e.g. Ethics hotline that uses a US service provider – notify employees of that fact

3. Building privacy into technology and procedures

Case study

- Voice Identification Service (VIS)

Bell's business challenge with identity

- Unlike financial services, most Bell services are for the household, but one individual is accountholder with possible co-users
- How do we know our customer's identity today?
  - no face to face relationship with our customers
  - identify them with shared public and private data over different channels
    - IVR, internet, retail, live agent, field forces
- Built out many different customer identification processes over the years and across different channels, e.g.
  - IVR – separate PIN for self serve of Bell Canada home phone services, Sympatico agent, ExpressVu
  - Unique personal PIN/password at live agent levels
  - www.bell.ca web site username and password
- IVR channel PIN/Postal Code identification is not transferred to live agent channels
  - Agents must re-identify customers
  - No consistent process across all live agents

Possible solutions to the challenge

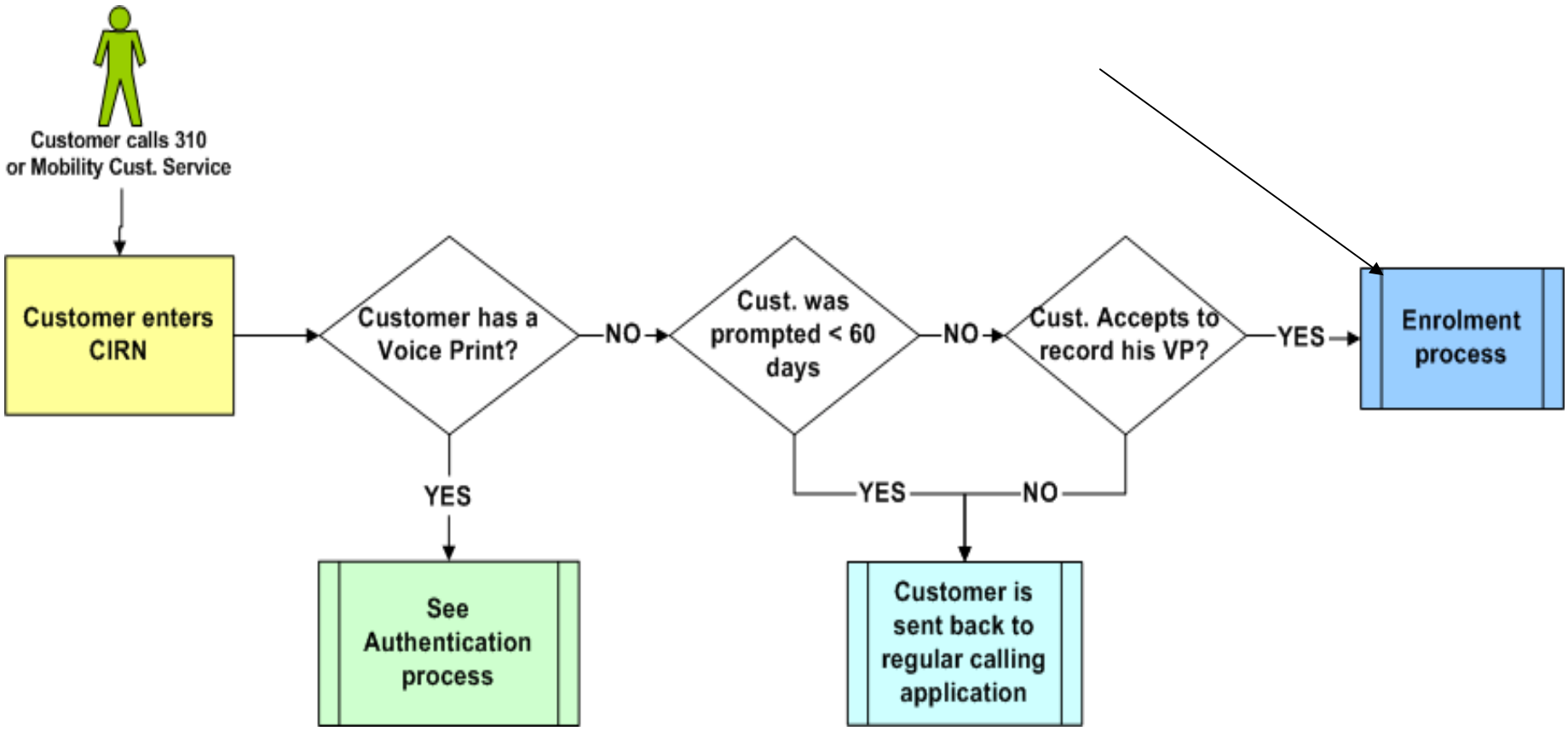
- We looked at a Universal PIN solution first
  - Our ExpressVu customers already used a 4 digit numeric PIN for this kind of identification in the IVR and in the call centre
  - Determined that PIN solution was too costly to maintain since customers could not remember their PIN in the current situation

- We next looked at a Speaker Verification solution
  - We had existing experience internally with this technology for field services technicians with positive results
  - Did a proof of concept to check for a secure solution, integration ease, flexibility in customer experience
  - Looked at using the customer phone number as a pass phrase
    - Chose to use a universal pass phrase instead
      - “At Bell, my voice is my password”

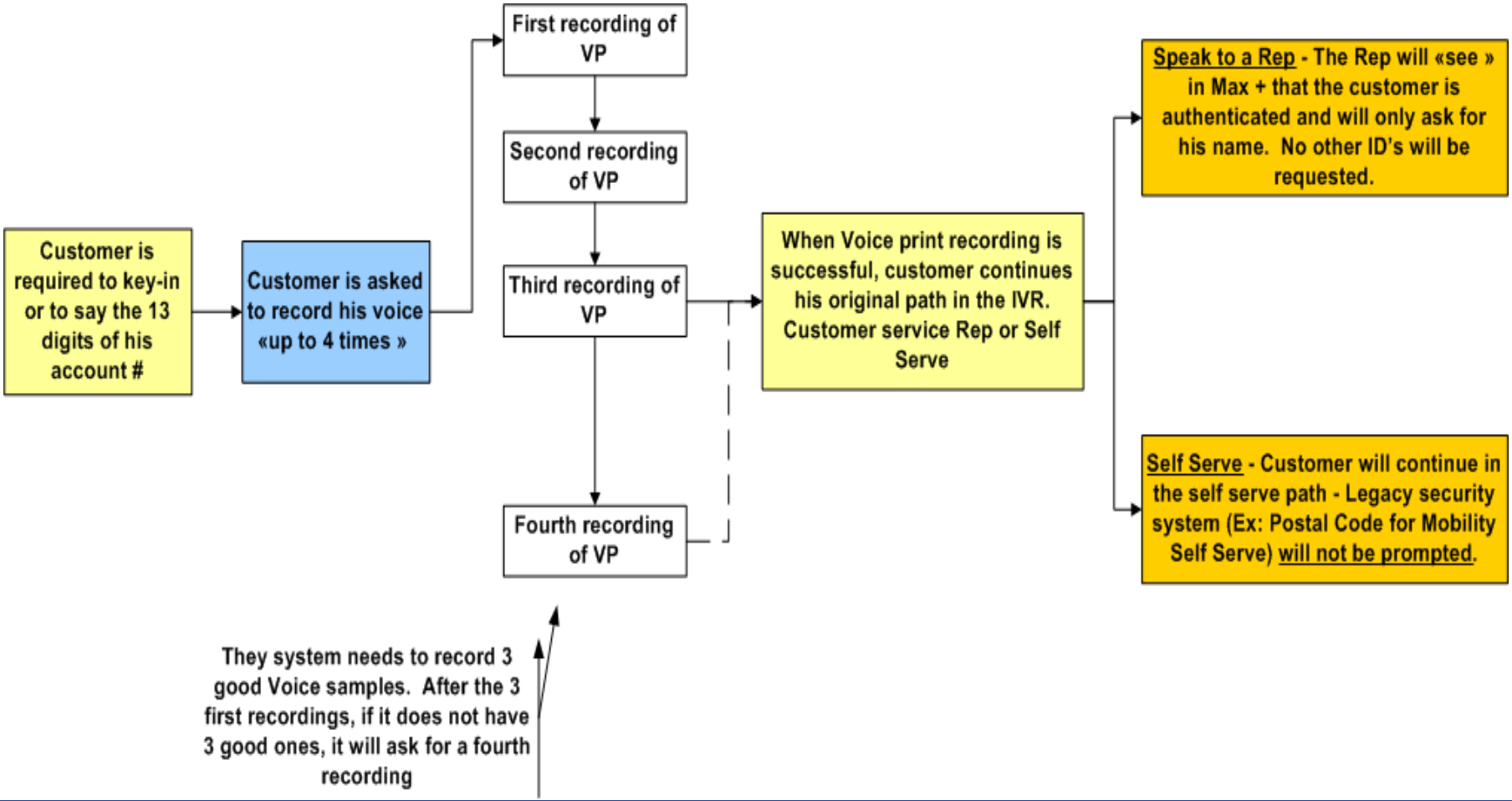
Voice Identification Service Design

- Considerations in Design for the IVR
  - Insert new identification process into current business logic
  - Customer choice to enrol with opt-out or re-prompt for enrol after 60 days
  - Opportunity for agent to send customer into IVR to enrol
  - "Calling In Regards to Number" (CIRN) is checked for enrolment in secure back end database in our corporate data centre
  - Have Calling Line ID as an audit with CIRN and account number as identification input that must match to proceed with enrolling a voice print against the account
    a) CLID - calling from – public) 2 and 3 must match to proceed
    b) CIRN - calling about – public) 1 is there for audit purposes
    c) Acct. # - shared - private)
  - Successful Verification allows customer to proceed in IVR through self serve or transfer to agent
  - Multiple voice prints per account are allowed for authorized account holder's and co-users
  - Successful enrolment requires a minimum of 3 audio inputs to complete a voiceprint

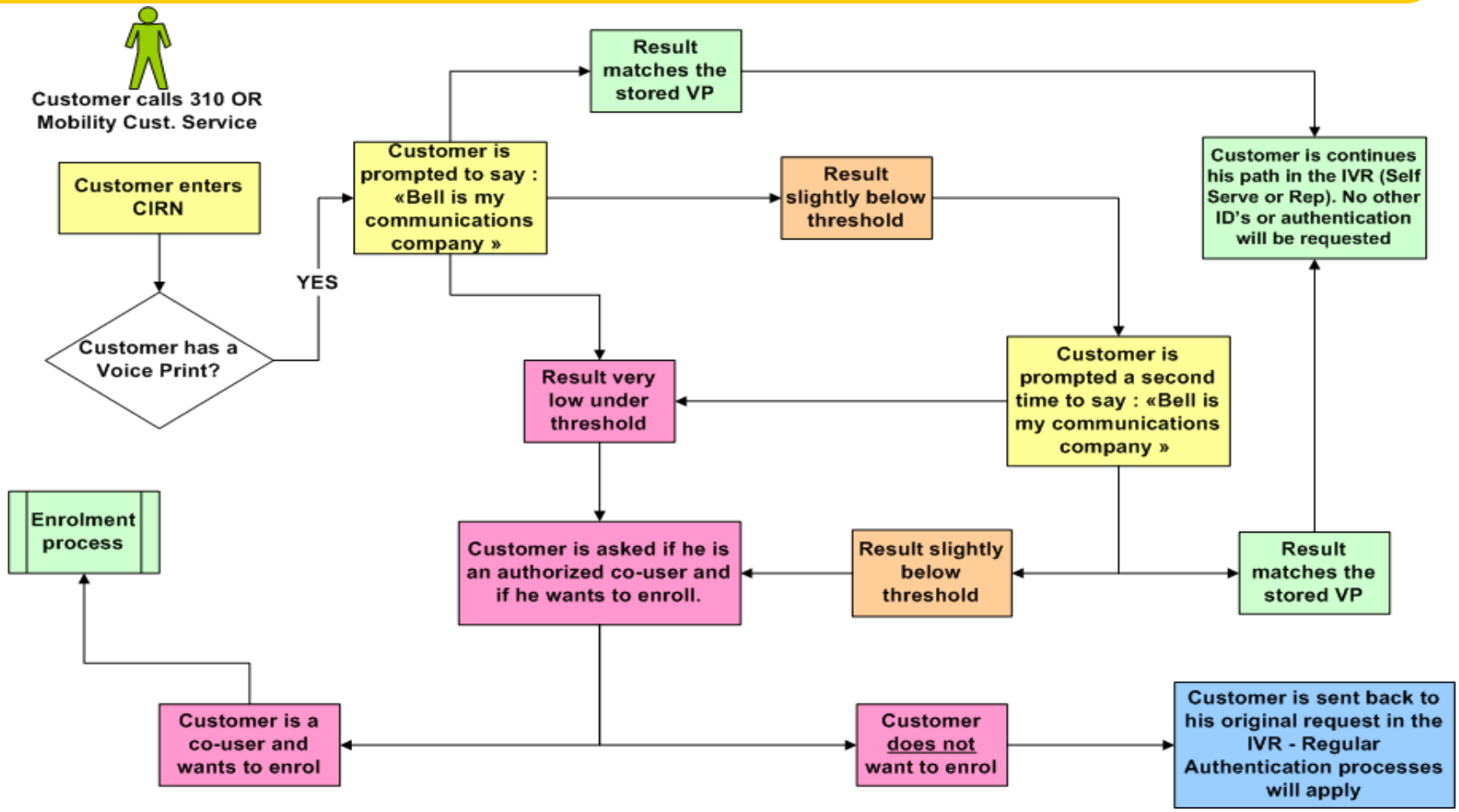
IVR Voice Print Process Begins



IVR Voice Print Enrolment Process



IVR Voice Print Authentication Process



Technology solution addresses challenge

- Safeguards
  - Agent has final accountability on calls transferred to determine individual identity of caller
  - Low business risk self serve in consumer market
  - Support “gui” is password protected
  - All logs are encrypted – reporting through “gui” only
  - Site specific encrypted key – can’t use our Bell solution anywhere else
  - SOx compliant data centres
  - Encryption of voice print related data
  - Stored in Bell’s secure data centres in Canada
  - Auto IVR call back to CIRN if enrolment completed against account, with info and agent support if required

Voice Identification Service - Deployment

- Why did we choose a pass phrase?
  - It's the best customer experience in a business model where we know our customers at the account level
    - they can have multiple accounts and phone numbers
    - multiple people can have authority on the same account
  - Easy to perform the verification
    - no customer memory load – we tell them what to say every time

It’s all about balance

balancing the demands of our customers for legitimate, timely access to their account information

with

the need to protect that information from unauthorized disclosure