

Vermont Crime On-Line

Privacy Policy

Table of Contents

Policy Statement	1
Definitions	1
Section 1: Purpose	2
Section 2: Collection Limitation.....	3
Section 3: Data Quality.....	4
Section 4: Use Limitation.....	4
Section 5: Security Safeguards	5
Section 6: Openness	6
Section 7: Individual Participation	7
Section 8: Accountability.....	7
Attachment Privacy Principles	8

Policy Statement:

It is the policy of the Vermont Department of Public Safety/Division of Criminal Justice Services/Vermont Criminal Information Center (VCIC) to protect *personal identifiable information* through the development of policies authorizing collection, use, processing, and dissemination of personal identifying information within the databases controlled by VCIC. Specifically, data which is characterized as **personal identifiable information** within the Vermont Crime On Line (VCON) database will not contain traditional identifying information such as name, date of birth, address, social security number, telephone number etc. The privacy design principles developed by the Organization of Economic Cooperation and Development's fair information practices shall be used to guide this policy development wherever applicable.

Definitions:

Accuracy of information – refers to adhering closely to data entry standards established by the Vermont Criminal Information Center, the FBI, and the Vermont Incident Based Reporting System (VIBRS) Advisory Board for the purpose of maintaining the integrity of exact crime information and decreasing the number of errors within the database.

Agency – An agency as used in this policy is a department that has a federal ORI number and whose mission/purpose/focus is the investigation of criminal activity.

Disseminate – To provide, release, or distribute information from the VCON system to anyone.

DPS – For the purposes of this policy DPS refers to the Vermont Department of Public Safety, Division of Criminal Justice Services/ Vermont Criminal Information Center.

Personal identifying information – Personally identifiable information is one or more pieces of information, when considered together, or combined with other information, and when considered in the context of how it is presented or how it is gathered, is sufficient to identify a unique individual. The pieces of information can be a) personal characteristics,¹ b) a unique set of numbers or characters assigned to

¹ *Personal Characteristics* includes such things as height., weight, gender, sexual orientation, date of birth, age, hair color, eye color, race, ethnicity, scars, tattoos, gang affiliation, religious affiliation., place of birth, mother's maiden name, distinguishing features, and biometric information such as fingerprints, DNA, retinal scans , etc.

a specific individual,² c) descriptions of event(s) or points in time,³ or d) descriptions of location(s) or places.⁴

User – For the purposes of this policy, a user is an individual who accesses the VCON system.

Section 1:

Purpose – What personal identifying information are we collecting and is it pertinent to the stated purpose?

The purpose Vermont Crime On-Line (VCON) is to provide both the public and criminal justice personnel with on-line crime information which is compliant with the FBI's National Incident Based Reporting System (NIBRS) in order to facilitate crime analysis at the local, regional, and statewide level.

In order to facilitate the analysis of crime and victimization patterns, VCON collects the following personal identifiers for individuals identified in police reports as offenders or crime victims:

- Age
- Gender
- Race
- Ethnicity
- Resident Status
- Relationship Between Victim and Offender

² A unique set of numbers or characters assigned to a specific individual includes such things as name, address (home or work), phone number(s), social security number, e-mail addresses, driver's license number, financial account or credit card number and associated PIN number, AIFIS, booking or detention system number,

³ Descriptions of event(s) or points in time includes information in documents such as police reports, arrest reports, medical records, etc.

⁴ Descriptions of location(s) or places includes such things as GIS locations, electronic bracelet monitoring information, etc.

Section 2:

Collection Limitation – Do we collect

personal identifying information unnecessarily?

Crime analysis involves the: 1) identification of crime patterns, trends, and problems; 2) the analysis of these patterns, trends, and problems; and 3) the dissemination of this information to criminal justice departments, governmental agencies, researchers, and the public in order to develop tactics and strategies to solve crime patterns, trends, and problems.

Crime analysis requires the study of patterns involving offenders, crimes, victims, time factors, location, modus operandi, and motivation. That is, crime analysis involves the “who, what, when, where, why, to whom, and how of crime”. Because crime analysis focuses on statistical patterns it is not necessary to collect information which identifies particular individuals, crime incidents, or addresses. **As such the only information collected by VCON regarding individuals is standard demographic information (e.g., age, gender, race, relationship etc.) related to the analysis of crime patterns.**

Though there are no names, addresses, or personal identifying numbers which can be used to identify victims or arrestees collected for the VCON System, it is possible in some small jurisdictions to identify personal information regarding a victim (e.g., age, race, relationship to the offender etc.) based on data available in VCON. For example, if a user of the system knew that Jane Doe was the victim of an assault in her town of residence during July of 2004, and Jane’s town of residence had only a limited number of assaults during that period, the user could determine Jane’s age and the fact that the offender in that incident was her husband. In order to prevent this inappropriate invasion of privacy, victim data on the VCON site is only available to the public at the state level. This decision to restrict public access was made in consultation with victim organizations throughout the state. Law enforcement personnel, however, have permissions to view victim data at the state, regional, and local level. Law enforcement access is only granted to law enforcement personnel who have signed a User Agreement with the Department of Public Safety and have been issued a secure account which is only accessible by using a user name and password. Secure account logins must be authenticated against a server at the Department of Public Safety before access is provided.

It would also be possible to identify certain personal identifying information regarding arrestees (e.g., age, gender, ethnicity, race, resident status) from VCON if a user of the system knew the particulars of a crime and the crime was committed in a jurisdiction where only a few crimes of a particular type were reported. Personal identifying information regarding arrestees, however, is a matter of public record and is available from a variety of sources including the media. As such, no special viewing restrictions were placed on this data.

Section 3:

Data Quality – How is the accuracy, completeness and currency of personal identifying information verified?

The data available on VCON were provided by municipal, sheriff, state police, and other Vermont state law enforcement agencies which are solely responsible for the accuracy of their submissions. Agencies are required to utilize automated editing software to error check their data prior to submitting the information to the Vermont Crime Information Center (VCIC). The FBI performs similar edit checks on Vermont's data before including the data in the national system. The data which appears in VCON has undergone edit checking at both the local and federal level before being published.

Staff at VCIC conducts a series of auditing procedures on the VCON data to ensure accuracy. VCIC also conducts quarterly training programs for contributing agencies which is informed by the auditing process.

The staff at the Vermont Center For Justice Research works closely with VCIC staff to load the crime data reported by law enforcement agencies into the VCON system. Prior to making the data available to the public, a series of statistical tests are performed against VCON by the Vermont Center For Justice Research to insure that the software is generating accurate reports.

Data will be updated on the VCON system on a quarterly basis.

Section 4:

Use Limitation – Is personal Identifying

information going to be used for anything other than what has been stated in the purpose of Vermont Crime On Line?

Information that is available on VCON is designed to be used for the purpose of providing both the public and criminal justice personnel with on-line crime information which is compliant with the FBI's National Incident Based Reporting System (NIBRS).

It is the intent of the VCIC that VCON data be used to facilitate crime analysis at the local, regional, and statewide level. It is, however, likely that VCON will be used for purposes other than crime analysis. For example, VCON information may be used

by researchers to construct quality of life indicators, by home buyers, or by insurance companies to assess risk. There is, however, no personal identifying information available from VCON beyond the statistical demographic information previously discussed. Therefore, regardless of the purpose to which VCON is put by users, there is no personal identifying information such as name, address, or other identifying numbers associated with VCON which can be misused.

Section 5:

Security Safeguards – What security

safeguards are in place to ensure that access to any personal identifying information or access to any of the crime data is not reached by unauthorized personnel or that it can not be tampered with?

There is no personal identifying information associated with VCON beyond statistical demographic data such as age, gender, and race. Thus there are no concerns that an unauthorized user can access personal identifying information.

The concern for VCON is to ensure that the data in the system is protected from tampering. Towards this end the following security measures have been taken: 1) the server is protected from unauthorized access by multiple layers of security including firewall and restricted physical access to the server; and 2) industry best practices are utilized to implement secure settings for the server and applications.

Section 6:

Openness – How does the Vermont Department of Public Safety collect, maintain, and disseminate the information contained in Vermont Crime On-Line?

The crime data provided for Vermont Crime On-Line is an enumeration of crimes known to law enforcement agencies. Crimes that are included in VCON are based on reports received by law enforcement agencies from victims, officers who discover infractions, or other sources. Crimes that may have occurred but were not reported are not included in this report. All reports of crime have been validated by a law enforcement officer. That is, reports which are later shown to be unfounded (e.g., property reported as stolen but later discovered as misplaced) are **not** included in VCON.

The data available through VCON were provided by municipal, sheriff, state police, and other Vermont state law enforcement agencies which are solely responsible for the accuracy of their submissions. All agencies were required to submit crime data for Group A and Group B crimes as defined by the Federal Bureau of Investigation's (FBI) National Incident Based Reporting System (NIBRS) program. The definitions for Group A and Group B crimes are accessible from the Vermont Crime On-Line site.

Agencies are required to utilize automated editing software to error check their data prior to submitting the information to the Vermont Crime Information Center (VCIC) and the Information Technology (IT) Section at the Department of Public Safety. The IT section collates the data from all reporting agencies and subsequently forwards the data to the FBI. The FBI performs similar edit checks on Vermont's submission before including the data in the national system. The FBI serves as the repository for Vermont's NIBRS data set and functions to update and modify records as additional information becomes available on cases.

Periodically VCIC requests downloads from the FBI and with the assistance of the Vermont Center For Justice Research assembles the data and loads it into VCON. A series of statistical tests are performed against VCON by the Center to ensure that the software is generating accurate reports. When VCON becomes a mature system data will be updated to the system on a quarterly basis.

The information that is available from VCON is distributed via a publicly accessible internet site. The location of this site is available from the Department of Public Safety Web Site (www.dps.state.vt.us).

Section 7:

Individual Participation – Is there any way for individuals to access their personal identifying information contained in the Vermont Crime On-Line?

There is no personal identifying information associated with VCON beyond statistical demographic data such as age, gender, and race. As such there is no way for an individual to access their personal identifying information.

If a member of the public questions the accuracy of information within the VCON system they may contact the NIBRS Auditor at the Vermont Crime Information Center (802-244-8727). The NIBRS Auditor will work with the complainant to resolve the error. Typically, resolution of data quality errors involves a referral to the originating agency that contributed the information.

Section 8:

Accountability – How is the Vermont Department of Public Safety going to oversee and enforce the provisions of this policy?

The Director of the Vermont Crime Information Center will be responsible for overseeing and enforcing the provisions of this policy. Oversight/enforcement will be accomplished by:

- Conducting quarterly checks on data quality.
- Verifying on a quarterly basis that privacy protection features are operational.
- Monitoring notifications of attempted unauthorized internet access.
- Investigating complaints from the public.
- Conducting training programs.
- Seeking feedback from users at training programs.

Max Schlueter, Ph.D
Director
Vermont Crime Information Center
Department of Public Safety
September, 2005

Attachment

Privacy Principles

The following eight privacy design principles provide a framework for developing privacy policy for a justice information system and for identifying technology requirements:

1. *Purpose Specification.* This principle requires identification of the purpose for which personal information is collected—in writing and not later than the time of data collection. The personal information collected should be pertinent to the stated purposes for which it will be used.
2. *Collection Limitation.* Agencies are to carefully review how they collect personal information to avoid collecting such data unnecessarily. Personal information should be obtained by lawful and fair means.
3. *Data Quality.* This principle mandates that agencies verify the accuracy, completeness, and currency of personal information.
4. *Use Limitation.* Personal information is not to be used or disclosed for purposes other than those specified in accordance with principle 1 above, except with the consent of the data subject, by authority of law, for the safety of the community, or pursuant to a public access policy.
5. *Security Safeguards.* Agencies must assess the risk of loss or unauthorized access to personal information in their systems. Reasonable safeguards against risks should protect personal information against loss or unauthorized access, destruction, use modification, or disclosure.
6. *Openness.* The principle requires agencies to provide notice about how they collect, maintain, and disseminate information. Openness also includes public access to establish the existence of personal data and to the data pursuant to an official public access policy.
7. *Individual Participation.* Agencies are to allow affected individuals to access their personal information.
8. *Accountability.* Agencies must have a means to oversee and enforce the other seven privacy design principles.